# Funktionelle Diversität mit asymmetrisch angeordnetem Vergleich und ihr Einsatz zur Lenkwinkelerfassung

DISSERTATION

zur Erlangung des akademischen Grades eines

DOKTORS DER NATURWISSENSCHAFTEN

(Dr. rer. nat.)

durch die Fakultät für Wirtschaftswissenschaften im Fach Informatik der


Campus Essen

vorgelegt von

Jan-A. R. Edel

Limburg / Lahn

Essen 2015

| | |
|---|---|
| Tag der mündlichen Prüfung: | 29.09.2016 |
| | |
| Erstgutachter: | Prof. Dr. Klaus Echtle, Universität Duisburg Essen |
| Zweitgutachter: | Prof. Dr.-Ing. Stefan Kowalewski, RWTH Aachen |

## DANKSAGUNGEN

Die vorliegende Dissertation, berufsbegleitend über viele Jahre entstanden, beruht auf dem Zusammenwirken vieler Umstände, der großartigen Unterstützung von Wissenschaftlern und Kollegen und nicht zuletzt auch auf dem Rückhalt in meiner Familie. Es ist mir daher ein großes Bedürfnis, mich bei allen zu bedanken, die in jeglicher Form zum Gelingen dieser Arbeit beigetragen haben.

Zunächst gilt mein Dank meinem Doktorvater, Herrn Prof. Dr. Klaus Echtle für die Übernahme des Hauptreferates. Daneben möchte ich Herrn Prof. Dr. Dr. Wolfgang A. Halang von der Fernuniversität Hagen danken. Auch durch ihn genoss ich über Jahre wertvolle Unterstützung und akademischen Rat. Ich danke ihm für die zahlreichen, kreativen Gespräche, für alle Anregungen, Meinungen und Ratschläge, welche mir stets eine große Hilfe waren und mit welchen meine Arbeit gut vorankommen konnte. Auch Prof. Dr.-Ing. Stefan Kowalewski von der RWTH Aachen bin ich für alle Unterstützung und das Zweitgutachten zu Dank verpflichtet.

Zu danken habe ich aber auch vielen meiner Kollegen, vor allem denen bei der Firma Leopold Kostal GmbH & Co. KG, einem der führenden Zulieferer von Lenkwinkelmesssystemen in der Automobilindustrie mit Hauptsitz in Lüdenscheid. Durch die intensive Zusammenarbeit mit ihnen, stellvertretend nenne ich Dr.-Ing. Michael Koepke, konnten bei damaligen Vorarbeiten wertvolles Wissen, viel Erfahrung und spannende Ideen erörtert werden und einfließen. Detailwissen zu Hall-Sensorik-Schaltkreisen verdanke ich der Kooperation mit Matthieu Poezart und seinen Kollegen in Bevaix in der französischen Schweiz, die bei der Firma Melexis N.V. mit Hauptsitz in Tessenderlo in Belgien tätig sind.

Meiner ganzen Familie danke ich für den steten Rückhalt sowie meiner Frau Clara, die durch ihre liebevolle Unterstützung einen wesentlichen Beitrag leisteten und mir die nötigen Freiräume zur Durchführung dieser Arbeit schufen.

Als besonderen Erfolg würde ich es betrachten, wenn mir in einer Welt elektronischer Funktionen mit dieser Arbeit auch ein Schritt zu mehr Sicherheit für unser menschliches Leben geglückt sein sollte.

Lüdenscheid, im November 2015

Jan-A. Reiner Edel

„Es wird Wagen geben, die von keinem Tier gezogen werden
und mit unglaublicher Gewalt daher fahren.“

Leonardo da Vinci - Erfinder und Ingenieur (1452 - 1519)

# INHALTSVERZEICHNIS

# ABKÜRZUNGEN

| | |
|---|---|
| 2oo3 | two out of three, zwei aus drei; sicherheitstechnischer Auswahlmechanismus |
| AAV | Asymmetrisch angeordnete Vergleichseinrichtung |
| ABS | Antiblockiersystem |
| ACC | Adaptive Cruise Control |
| ADC | Analog-to-Digital Converter |
| ADS | Audi Dynamic Steering (Audi) |
| AFS | Adaptive Front Steering (BWM) |
| AHS | Automatischer Heckspoiler |
| ASG | Antriebsstrang Steuergerät |
| ASIL | Automotive Safety Integrity Level |
| ASP | Analog Signal Processing |
| ATAN | trigonometric function: arctangent (or inverse tangent) |
| AUTOSAR | AUTomotive Open System Architecture |
| BGB | Bürgerliches Gesetzbuch |
| BIST | Built-In Self Test |
| Byte | 8 Bits |
| bzgl. | bezüglich |
| bzw. | beziehungsweise |
| CAD | Computer-Aided Design, engl. für rechnergestützter Entwurf oder rechnergestützte Konstruktion |
| CAN | Controller Area Network |
| CC | Common Cause |
| CCA | Common Cause Analysis |
| CIM | Computer Independent Model |
| CM | Change Management, zu Deutsch: Änderungsmanagement (selten) |
| CM | Configuration Management, zu Deutsch: Konfigurationsmanagement |
| CMMI | Capability Maturity Model Integration |
| CMOS | Complementary Metal Oxide Semiconductor |
| COTS | Commercial off-the-shelf |
| CPU | Central Processing Unit |
| CRC | Cyclic Redundancy Code, Prüfsumme mit Polynomfunktion, Signatur |
| DAMUK | Definition, Analyse, Massnahmenentscheidung, Umsetzung, Kommunikation |
| DC | Diagnostic Coverage (Diagnoseabdeckung) |
| Die | Silizium-Substrat, Halbleitergrundfläche |
| DIN | Deutsches Institut für Normung e. V. |
| DIS | Draft International Standard |
| DNL | Differential Non-Linearity |
| DSP | Digital Signal Processing |
| E/E/PE | elektrisch/elektronisch/programmierbar elektronisch |
| ECC | Hamming Error Correction Coding |
| ECU | Electronic Control Unit |
| EDV | Elektronische Datenverarbeitung |
| E/E | Elektrik/Elektronik |
| EEPROM | Electrically Eraseable Programmable Read Only Memory |

| | |
|---|---|
| EFQM | European Foundation for Quality Management |
| EMC | Electro-Magnetic Compatibility |
| EMF | Eclipse Modeling Framework |
| en | englisch, auf Englisch |
| EPS | Electric Power Steering |
| ESD | Elektrostatic Discharge, Elektrostatische Entladung |
| ESP | Elektronisches Stabilitätsprogramm |
| ETA | Event Tree Analysis |
| EUC | Equipment Under Control |
| evtl. | eventuell |
| FA | Fehlerart |
| FDIS | Final Draft International Standard |
| FE | Falling Edge |
| FIT | Failure in time [$10^{-9}$/h] |
| FMEA | Failure Mode and Effect Analysis |
| FMECA | Failure Modes, Effects and Criticality Analysis |
| FMEDA | Fault Modes Effects, and Diagnostics Analysis |
| FMVSS | Federal Motor Vehicle Safety Standard |
| FPGA | Field programmed gate array |
| FS | Functional Safety, Funktionssicherheit |
| FSK | Funktionales Sicherheitskonzept |
| FTA | Fault Tree Analysis |
| FTTI | Fault Time Tolerance Interval |
| FuSa | Functional Safety (Funktionale Sicherheit) |
| FW | Firmware |
| Gauss (G) | Einheit für magnetische Flussdichte - 1 mT = 10 G |
| GPSG | Geräte- und Produktsicherheitsgesetz |
| Hall | Magnetischer Feldeffekt nach dem Entdecker E. Hall (1855-1938) |
| HiL | Hardware-in-the-Loop |
| HW | Hardware |
| IC | Integrated Circuit (integrierter Schaltkreis, IS) |
| IEC | International Electrotechnical Commission (Normungsgremium) |
| IMC | Integrated Magneto-Concentrator (IMC®) |
| INL | Integral Non-Linearity |
| ISO | International Standardisation Organisation (Normungsgremium) |
| KM | Konfigurationsmanagement |
| LF | Latent Fault (im System verbleibender, nicht beherrschter MPF) |
| LIN | Local Interconnect Network |
| LSB | Least Significant Bit |
| LWS | Lenkwinkelsensor, Lenkwinkelsensormodul |
| MC | Mikrocontroller |
| MPF | Multi Point Fault (Ausfall, der nur in Kombination mit anderen Ausfällen gefährlich werden kann) |
| MSB | Most Significant Bit |
| NC | Not Connected |
| NVP | N-Version Programming |

| | |
|---|---|
| OEM | Original Equipment Manufacturer |
| OSI | Open Systems Interconnection |
| PiUA | Proven in Use Argument |
| Pkw | Personenkraftwagen |
| PM | Projektmanagment |
| PMHF | Probabilistic Metric for random Hardware Failures |
| POR | Power On Reset (Neustart nach Anlegen der elektrischen Spannung) |
| PS | Power Supply (Energieversorgung mit Spannungsregler) |
| PWM | Pulsweitenmodulation, hier: pulsweitenmoduliertes Signal |
| QM | Qualitätsmanagement, en: Quality Management |
| QS | Qualitätssicherung |
| RAM | Random Access Memory |
| RE | Rising Edge |
| RF | Residual Fault (trotz Mechanismus verbleibender Ausfall, der ein Sicherheitsziel direkt verletzt) |
| RISC | Reduced Instruction Set Computer |
| RM | Requirement Management, zu Deutsch: Anforderungsmanagement |
| ROM | Read Only Memory |
| RTE | Realtime Environment (AUTOSAR), dt. Echtzeitumgebung |
| SAS | Steering Angle Sensor (LWS) |
| SCI | Serial Communication Interface (siehe auch SPI) |
| SEooC | Safety Element out of Context |
| SIL | Safety Integrity Level |
| sog. | sogenannt |
| SM | Sicherheitsmechanismus (en: safety mechanism) |
| SPF | Single Point Fault (Ausfall, der das Sicherheitsziel direkt verletzt) |
| SPI | Serial Peripheral Interface (siehe auch SCI) |
| SPICE | Software Process Improvement and Capability dEtermination |
| SRS | Software Requirement Specification, zu Deutsch: Softwareanforderungsspezifikation |
| SW | Software |
| SW-C | Software Component (AUTOSAR) |
| Sys | System |
| SysML | Systems Modeling Language |
| SZ | Safety Goal, zu Deutsch: Sicherheitsziel |
| TC | Temperature Coefficient (in ppm/Deg.C.) |
| Tesla (T) | Einheit für magnetische Flussdichte - 1 mT = 10 G |
| TQM | Total Quality Managmement (Methodik im QM) |
| TSA | Technische Sicherheitsanforderung |
| TSK | Technisches Sicherheitskonzept |
| UML | Unified Modeling Language |
| VDA | Verband der deutschen Automobilindustrie |
| vgl. | vergleiche |
| WD | Watchdog (Überwachungseinrichtung) |
| Word | Datenwort mit der Breite von 16 Bits (= 2 Bytes) |
| z.B. | zum Beispiel |

## KURZFASSUNG

Elektronik und Dutzende elektronische Steuereinheiten (ECUs) dominieren mittlerweile das Automobil und alle seine Funktionen. Ein Lenkwinkelsensormodul stellt beispielsweise verschiedensten Fahrzeugfunktionen die aktuelle Fahrtrichtung bereit. Fehlerbedingte Ausgabe falscher Winkel führt in einer verknüpften Assistenzfunktion mit eigenständiger Beeinflussung der Quer- und Längsdynamik des Fahrzeugs zu einem unvertretbaren Gefahrenrisiko. Zur Risikominderung werden sich bei Versagen gefährlich auswirkende Funktionalitäten gemäß der Norm ISO 26262 entwickelt. Dazu werden in dieser Norm unter anderem ein geeignetes Sicherheitskonzept und seine Anwendung gefordert. Um die höchste normgemäße Sicherheitsintegritätsstufe ASIL D zu erreichen, ist das altbewährte Sicherheitskonzept *EGAS* in aller Regel zu schwach, weil es nur ein nichtredundantes Rechnersystem (MC) vorsieht.

Unter der Bedingung, ebenfalls mit einem einzigen MC auszukommen, wird zur Lösung dieses Problems ein neuartiges Sicherheitskonzept entwickelt. Es sieht vor, von MC berechnete Ausgangsgrößen funktionell diversitär auf redundante Sensorgrößen umzurechnen. Die im zweiten Sensorbaustein integrierte und damit asymmetrisch angeordnete Vergleichseinrichtung (AAV) stellt unabhängig von MC und für jeden einzelnen von MC erarbeiteten Funktions- und Ausgabewert die Integrität sowohl der Daten als auch der Rechner- und Sensorhardware sicher. Weiterhin vereinfacht dieser Aufbau den Verifikationsaufwand entscheidend, weil weder Sensoren noch umfangreiche MC-Software, sondern allein die Funktion der weit weniger komplexen AAV verifiziert werden muss. Die Beschränkung auf neben MC nur zwei weitere integrierte Schaltungen (ICs) stellt ebenfalls eine für die funktionale Sicherheit vorteilhafte Vereinfachung dar, denn zwei gleiche, jedoch funktionell diversitär erfassende Sensor-ICs verringern die Komplexität des neuen Konzepts auf das Notwendigste. Im Gegensatz zum EGAS-Konzept ist allmähliche Leistungsabsenkung sowie Notlauf einzelner Funktionalitäten möglich. Dies wird durch von Ende zu Ende abgesicherte Freigabe- bzw. Abschaltbotschaften erreicht, die AAV nach Vergleichen unabhängig von MC an die Aktorik sendet. Im konkreten Einsatz zur Lenkwinkelerfassung wird demonstriert, wie bzw. dass die höchsten normativen Anforderungen an die Hardwaresicherheitsintegrität für eine ECU mit nur einem Rechnersystem erfüllt werden. Anschließend wird in einer tiefgreifenden und umfassenden Bewertung der Sicherheitsintegrität in Systemen mit dem vorgestellten Sicherheitskonzept verallgemeinernd seine Eignung für Fahrzeugfunktionalitäten mit Sicherheitszielen bis ASIL D gezeigt und nachgewiesen.

# 1 EINLEITUNG

## 1.1 UMFELD UND HERAUSFORDERUNG

Die Geschichte der Elektronik ist im Vergleich zur Entwicklungsgeschichte des Menschen noch sehr jung. Umso rasanter hat die Elektronik alle Bereiche des täglichen Lebens einnehmen können. Auch im Automobil ist Elektronik für fast alle Fahrzeugfunktionen längst sogar beherrschend geworden [1]. Für etwa neun von zehn Innovationen im Kraftfahrzeug werden heute elektronische Systeme eingesetzt [2]. Die aktuellen Trends zu neuen, umweltschonenden Technologien wie Elektromobilität, zu Fahrerassistenzsystemen oder gar zu hochautomatisiertem Fahren machen schnell klar, dass für diese neuen, elektrischen, elektronischen und softwarebasierten Systeme (E/E/PE Systeme) zudem höchste Sicherheitsanforderungen eingehalten werden müssen. Sie selbst wird mitunter auch sehr wirkungsvoll für alle möglichen Schutzfunktionen eingesetzt. Allerdings kann sie durch ihren Einsatz bei Versagen leider auch selbst zur Gefahr werden. Die rasant zunehmende Komplexität von elektronischen Schaltungen, Schaltungsvernetzungen mit Strukturen im Nanometerbereich oder auch von programmatischen Kodierungen dieser Elektronik (Software, SW) kann sogar kontraproduktiv zur Sicherheit für Leib und Leben sein.

Der Airbag zum Beispiel, der die Insassen bei einem Aufprall des Fahrzeugs schützen soll, verliert bei seinem Ausfall nicht nur seine eigentliche Schutzfunktion, sondern kann bei Versagen seiner Elektronik durch eine ungewollte Auslösung selbst zur Gefahr werden. Eine Elektronik, die zur Kontrolle oder sogar zur Steuerung der Lenkung dienen soll, kann das Fahrzeug bei unglücklichem Versagen in eine ungewollte Richtung lenken.

Genau diese Art Gefahren gilt es zu vermeiden, sodass die Sicherheit des Gesamtsystems *Fahrer mit Fahrzeug* durch den Einsatz von Elektronik nicht beeinträchtigt wird und nach Möglichkeit sogar steigt.

Die folgenden Teilabschnitte sollen weitere Aspekte der Problemstellung beleuchten.

### 1.1.1 KOMPLEXITÄT

Die stetige Suche nach Innovationen und Verbesserungen geht mit einem Zuwachs von Vernetzung und Komplexität einher. Auch im Fahrzeug scheint die Komplexität immer noch rasant zu wachsen, laut [3] und [4] in den Bereichen Sicherheit, Komfort und Unterhaltung. Es wird an einer Unmenge neuer oder verbesserter Fahrerassistenzfunktionen geforscht und entwickelt, die zunehmend aktiv in die Bewegung des Fahrzeugs eingreifen.

Einige solcher Systeme sind der Parkassistent [5], der Spurhalteassistent[1], der Toter-Winkel-Assistent [6] und der Bremsassistent [7].

Diese Systeme greifen immer selbstständiger in die Bewegung des Fahrzeugs ein, wobei Fahrerwunsch und Steuerbefehle unter Umständen überstimmt oder ignoriert werden. Beispiele hierfür sind automatisches Ausweichen [8], automatisches Rechts-Ran-Fahren [9] oder das Fahrzeug sicher zum Stehen zu bringen [10], wenn eine andere Funktion z.B. die Fahrunfähigkeit des Fahrers erkannt hat.

Alle diese Funktionen werden über ein Netz von sogenannten Steuergeräten für Sensorik, Logik und Aktorik realisiert. Funktion und Sicherheit wird auf mehrere Steuergeräte verteilt. Für Fahrzeuge der Oberklasse stellen 70 und mehr verbaute Steuergeräte heute keine Seltenheit dar [11]. Laut Bosch [12] waren bis 2004 zum Beispiel schon sieben verschiedenartige elektrische oder elektronische Komponenten (E/E) an der Erfüllung der adaptiven Fahrgeschwindigkeitsregelung (ACC) beteiligt. Die Komponenten sind zur Interaktion miteinander über Standard-Bussysteme des Automobilbereichs wie CAN, LIN, FlexRay und MOST vernetzt. Zur Erfüllung einer gemeinsamen Systemfunktion müssen im Zusammenspiel der einzelnen Komponenten oft harte Echtzeitbedingungen eingehalten werden.

Die Vernetzung von Steuergeräten unterliegt oft keiner eindeutigen Abgrenzung zu anderen Assistenzsystemen. Ein Steuergerät benötigt zur Realisierung einer Fahrerassistenzfunktion meist mehrere andere Steuergeräte und sonstige elektrisch/elektronische Komponenten und kann selbst ebenfalls auch Bestandteil völlig anderer Assistenzfunktionen sein.

Bei redundanter Plausibilisierung sicherheitskritischer Größen auf mehreren Steuergeräten kann sich ein sicherheitstechnisch positiver Effekt zeigen. Die Komplexität solcher Systeme jedoch steigt durch ihre Vermaschung zweifellos und macht die sichere Funktion der Systeme schwieriger.

Zudem basiert jedes Steuergerät (ECU), im Englischen *Electronic Control Unit* genannt, wiederum auf SW, und zwar auf verschiedenen Ebenen und für verschiedene Unterfunktionen bezüglich Netzkommunikation, Plausibilisierung, Signalnormierung, Logik, Regelung, Absicherung und Ansteuerung.

Ein einfaches Gedankenspiel soll verdeutlichen, wie exponentiell der Komplexitätszuwachs durch den Einsatz von SW aussieht. Hätte bei nur sechzehn der an einer Assistenzfunktion beteiligten ECUs jede einzelne nur 2 verschiedene Zustände, so ergäben sich dabei $2^{16}$ = 65.536 Kombinationsmöglichkeiten [13]. Das sind ebenso viele Möglichkeiten für einen Ausfall der Assistenzfunktion. Wäre nun jeder dieser zwei Zustände pro ECU

[1] Bei Daimler AG in Form selektiven Bremsens von Rädern über das ESP, welches eine Gier-Bewegung

durch ein kleines Softwaresystem von 10.000 Befehlszeilen (en: lines of code, LOC) realisiert und jede zehnte Programmzeile wäre ein bedingter Sprung, der das Programm je in einen weiteren Zustand aufgabelt, so ergäben sich hier bereits $2000^{16}$, also über $6{,}5*10^{52}$ einzelne Kombinationen möglichen Versagens. Die Realität ist in der Regel weit komplexer.

Sicherheitstechnisch stellt die durch alle diese Trends aufgespannte Komplexität zweifellos eine gewaltige Herausforderung dar und ist durch professionelle Entwicklung, Prozesse und Verifikation auf noch so hohem und formalem Niveau allein nicht beherrschbar. Je nach Kritikalität werden entsprechende technische Sicherheitskonzepte notwendig, die die Komplexität durch ihre Einfachheit und vor allem durch klare Redundanz bei sicherheitskritischem Versagen von Hardware (HW) beherrschbar machen.

### 1.1.2 KOSTENDRUCK

Die Automobilzulieferbranche mit ihren Massengütern auf hohem Preisniveau sieht sich seit jeher einem wachsenden Kostendruck gegenüber [14]. Jährliche Forderungen von manchmal pauschal 5% Preisnachlass von deutschen Autobauern an Zulieferer und die teils aktive Förderung zum Erhalt von konkurrierenden Markbegleitern machen dies sehr deutlich. Die permanente Erwartung nach Verbesserung der Qualität und Sicherheit erhöht den Druck zusätzlich. Angesichts nicht unüblich hoher Serien von beispielsweise einer Million Fahrzeugen mit jeweils bis zu 10.000 Einzelteilen, die zu etwa 80% zugeliefert werden müssen [15], wird schnell klar, wie sich jeder halbe Cent beim Einkauf von Material oder Bauteilen stark bemerkbar macht. Bei Produkten, die sicherheitsrelevant eingesetzt werden sollen, kommt man in der Regel um zusätzliche Kosten für die Absicherung der relevanten Funktionen nicht herum. Das sind unvermeidbare Aufwände für sicherheitsnormkonforme Entwicklungsprozesse und Bestätigungen sowie vor allem Kosten für zusätzliche Bauteile und redundante Ausführungen, die mit steigender Kritikalität einer Funktion zur Absicherung und Fehlerbeherrschung notwendig werden und mit steigenden Stückzahlen natürlich immer stärker ins Gewicht fallen. Die Kosten für zusätzlich einzusetzende HW könnten den Preis eines höchst sicherheitsgerichteten Systems im Automobil leicht verdoppeln, wenn man beispielsweise einmal von einer vollständigen HW-Redundanz für die eigentliche Funktion ausgeht. Geringe Kosten müssen aber der Sicherheit nicht widersprechen. Im Gegenteil kann gerade die Einfachheit eines Systems viel zur Sicherheit eines entsprechenden Produkts beitragen. Je weniger Elektronik zum Einsatz kommt, desto weniger Ausfälle sind im Vorfeld zu betrachten und desto einfacher, übersichtlicher und damit sicherer kann das System sein. Vor diesem Hintergrund kommt einem guten, technischen Sicherheitskonzept mit höchsten Ansprüchen an kompromisslose

Sicherheit besonders die Intelligenz von Einfachheit zugute. Diese ist sicherheitstechnisch generell förderlich und steht dem stupiden Einsatz von Bauteilredundanzen hinsichtlich der Kosten sogar entgegen.

### 1.1.3 GESETZGEBUNG UND PRODUKTHAFTUNG

Im Jahr 2010 veröffentlichte das Kraftfahrt-Bundesamt (KBA) eine Statistik, nach der mit 185 Rückrufaktionen ein neuer Rekord erreicht wurde. Noch zehn Jahre zuvor mussten die Hersteller im Vergleich nur 72-mal Fahrzeuge zurückrufen [16]. Anderen Quellen zufolge sinkt die Zahl der Rückrufe. Zumindest in Deutschland habe sich die Zahl seit 2007 von seinerzeit 157 auf etwa 140 im Jahr 2010 reduziert [15]. Sicher ist jedenfalls, wahrscheinlich auch durch vermehrte Berichterstattung, eine erhöhte Aufmerksamkeit und Sensibilität der Verbraucher. Dadurch sinkt natürlich die gesellschaftliche Akzeptanz für Gefahren und Risiken, die von Fahrzeugelektronik ausgehen.

Zudem scheinen sowohl die vorangehenden Auswirkungen mit Verletzten und Todesopfern dramatischer zu werden, als auch die Ausmaße der Aktionen über gewaltige Serien anzusteigen. Das Beispiel Gaspedal-Rückruf eines führenden japanischen Herstellers wie auch die jüngsten Rückrufaktionen mit mehreren Millionen Zündschlössern des größten amerikanischen Autobauers zeigen dies eindrucksvoll. Das Vertrauen der Kunden in zurückgerufene Produkte der Automobilhersteller kann schnell beschädigt werden, insbesondere, wenn diese aufgrund bestehender, ernsthafter Gefahr für Leib und Leben von Verkehrsteilnehmern auffällig werden.

Rückrufaktionen oder gar Verfahren vor Gericht machen – abgesehen von möglicherweise vernichtenden Schäden des Ansehens eines Herstellers - die im Feld gefundenen Designfehler zu den teuersten. Sie sollten also auch wirtschaftlich gesehen die Motivation unterstützen, Fehler und Sicherheitslücken möglichst früh im Entwicklungsprozess aufzuspüren.

Nach einem ersten Unfall werden in der Regel die Schuldigen gesucht und unter Umständen auch schnell gefunden. Dann droht möglicherweise sogar strafrechtliche Verfolgung. Die gesetzlichen Grundlagen für Deutschland hierfür liegen im §823 BGB und §1 Abs.1 des Produkthaftungsgesetz (ProdHaftG). Demnach muss ein Hersteller, der seine Produkte in Verkehr bringt, bei bestimmungsgemäßer Verwendung, aber auch bei vorhersehbarer Fehlanwendung, die Sicherheit und Gesundheit der Kunden sicherstellen. Für entstandenen Schaden ist er zu Schadensersatz verpflichtet. Auch das geltende EU Recht steht mit dem Geräte- und Produktsicherheitsgesetz (§4 GPSG) in Harmonie dazu.

Frei von Schuld und Ersatzpflicht kann nach §1 Abs.2 ProdHaftG nur derjenige Hersteller sein, der den Produktfehler oder die Sicherheitslücke zum Zeitpunkt des

Inverkehrbringens nicht erkennen konnte und der Stand der Wissenschaft und Technik bis dato eingehalten wurde. Dies wiederum könnte vor Gericht sehr leicht durch eine Nicht-Konformität zu den betreffenden Normen widerlegt werden. Kann der Hersteller dem Produkthaftungsrichter eine akkreditierte Bestätigung zur Einhaltung der ISO26262 für seine sicherheitsrelevante Funktion im Fahrzeug vorlegen, dreht sich die Bürde des Beweises von Unschuld zu Lasten des Geschädigten um, was juristisch Beweislastumkehr genannt wird. Mit dem Konformitätsnachweis ist dann der Geschädigte in der Pflicht, einen Beweis für die Schuld des Herstellers zu erbringen, zum Beispiel Fahrlässigkeit an einer ganz bestimmten Stelle. Beweislast, ob für den Geschädigten oder für den Produkthersteller ohne Normenkonformität kann sich beliebig schwierig bis unmöglich gestalten [16] und führt in der Regel, wie erwähnt, sehr schnell zum Nachsehen vor Gericht.

### 1.1.4 FUNKTIONALE SICHERHEIT UND NORMEN

Mit funktionaler Sicherheit (auch Funktionssicherheit, en: functional safety, FS) ist der Teil der Gesamtsicherheit gemeint, der von der korrekten Funktion insbesondere elektrischer, elektronischer und programmierter Elektronik (E/E/PE) abhängt, um Schäden, vor allem für Leib und Leben, abzuwenden [17].

Ein sicherheitsbezogenes System ist ein System, das eine oder mehrere Funktionen zur Umsetzung der Anforderung nach funktionaler Sicherheit besitzt und bei deren Versagen gefährliche Auswirkungen die Folge wären [18]. Generell sind die Begriffe um funktionale Sicherheit vielfältig und manchmal nicht leicht voneinander abzugrenzen. Sicherheitsbezogen, sicherheitsgerichtet und sicherheitsrelevant wird z.B. oft synonym verwendet. Die englischen Entsprechungen *safety related*, *safety aligned* oder *safety relevant* machen die Sache nicht klarer. Dennoch hat man sich bei mancher internationalen Normengebung darauf verständigt, die Problematik klarer Begrifflichkeiten nicht dadurch zu verschärfen, die in Englisch entstandene Fassung in nationalsprachliche Fassungen zu überführen.

Als sogenannte Basisnorm für funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer, programmierbar elektronischer Systeme wurde erstmalig im Jahr 1998 die internationale Norm IEC 61508 veröffentlicht. Aktuell liegt sie in einer revidierten und erweiterten Form als zweite Ausgabe aus dem Jahr 2010 vor [19]. Von dieser Norm ausgehend wurden bereits und werden verschiedene sektorspezifische Normen abgeleitet.

Für den Automobilbereich und E/E/PE Systeme in Straßenfahrzeugen bis 3,5 Tonnen Zulassungsgewicht ist dies die ISO 26262 [20], die aus oben genannten Gründen übrigens nur Englisch vorliegt.

Bei den Sicherheitsnormen üblich ist eine Einteilung der definierten Anforderungen nach Anforderungs- und Risikoklassen. Im Automobilbereich werden mit der ISO 26262 **A**u-

tomotive **S**afety **I**ntegrity **L**evel (ASIL) A bis maximal D zugeordnet, um die verschiedenen Sicherheitsziele (SZ, en: safety goal) des betrachteten Systems in Klassen mit steigendem Sicherheitsrisiko zu unterteilen. Ab einem ASIL A gehen die Anforderungen der ISO 26262 zur Reduzierung des Sicherheitsrisikos über die eines Qualitätsmanagementsystems hinaus. Die Methoden und Prozessanforderungen von Qualitätsnormen und –modellen reichen alleine nicht aus [21]. Die Anforderungen der Sicherheitsnormen richten sich zum großen Teil an die Prozesse und die Methodik zur Entwicklung solcher Systeme und werfen dort einen gewissen Mehraufwand gegenüber anderen Entwicklungen auf. Ein anderer Teil von Sicherheitsanforderungen für höhere Sicherheitsintegritätsstufen (SIL/ASIL) zielt auf ein geeignetes Sicherheitskonzept mit dem Einsatz von zusätzlicher HW für Diagnose und Redundanz zur Fehlerbeherrschung im Betrieb solcher Systeme ab. Während zur Erreichung eines SZs auf ASIL A gegebenenfalls noch eine um entsprechende Anforderungen der ISO 26262 erweiterte Methodik ausreicht, werden für kritischere SZs neben entsprechend höheren Ansprüchen im systematischen Bereich auch zunehmend mehr technische Sicherheitsmechanismen notwendig.

### 1.1.5 Entwicklungsprozesse und Methoden versus Mechanismen

Funktionale Sicherheit ist eine Produkteigenschaft. Sie muss aktiv eruiert und auch konstruktiv entwickelt werden. Die Anforderungen an das Erreichen von funktionaler Sicherheit können grob zwischen Prozessanforderungen und Produktanforderungen unterschieden werden. Prozessanforderungen sind Anforderungen der Norm, die sich mit den Anforderungen von Qualitätsmanagementsystemen überdecken und darüber hinausgehen. Abbildung 1.1 soll die unterschiedlichen Anforderungsbereiche und mögliche Überschneidungen im Bereich von Prozessanforderungen am Beispiel für Softwareentwicklung verdeutlichen. Prozessanforderungen betreffen Sicherheitskultur, Methodik, bestimmte Inhalte von Arbeitsprodukten oder bestimmte Aktivitäten, also die Systematik bei der Produktentstehung und insbesondere schon bei der Entwicklung des Produkts. Produktanforderungen hingegen können notwendige Eigenschaften des Produkts selbst, zum Beispiel zur Selbstüberwachung sein. Diese technischen Eigenschaften werden in der Regel durch die Architektur und durch Sicherheitsmechanismen erreicht, die mittels zusätzlicher Bauteile oder per SW aufgebaut werden.

Hinter dem richtigen systematischen Ansatz bei den Entwicklungsprozessen, mit dem von Anfang an systematische Fehler vermieden werden sollen, beschäftigen sich die technisch zu realisierenden Anforderungen an das Produkt der Beherrschung von kritischen Ausfällen und Fehlern, die später spontan im Betrieb auftreten könnten.

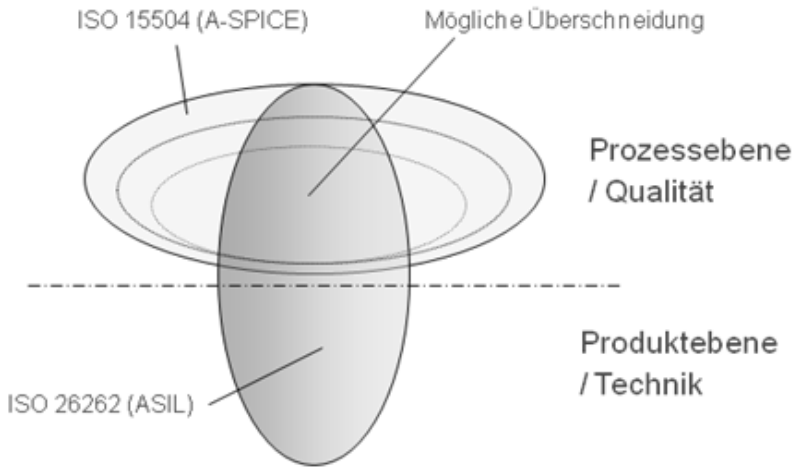



Abbildung 1.1: Mögliche Überschneidung von Sicherheits- und Qualitätsmanagementanforderungen im Bereich der Entwicklung von SW.

Vom Entwicklungsingenieur wird neben der Einhaltung einer Sicherheitskultur und eines damit verbundenen Vorgehens auch im technischen Bereich ein entscheidender Beitrag zur funktionalen Sicherheit erwartet. Funktionale Sicherheit bedeutet hier, ausgehend von SZs für eine Funktionalität ein Sicherheitskonzept, technische Maßnahmen und Sicherheitsmechanismen zu entwickeln, um fehlfunktionsbedingte Gefährdungen zu beherrschen, abzuwenden oder besser gar nicht erst entstehen zu lassen. In der üblicherweise über etliche Zulieferer verteilten Entwicklung einer Fahrzeugfunktionalität sind Hierarchie, Modularität und Kapselung wichtige Prinzipien für Architektur und Entwurf, die insbesondere auch für das Konzept von Sicherheitsmechanismen gelten.

Der eine, systematische Ansatz über geeignete Entwicklungsprozesse darf gegen den Ansatz der Fehlerbeherrschung natürlich nicht ausgespielt werden. Beide Ansätze sind komplementär, weil sie sich bei der Absenkung der verschiedenen Risiken im Hinblick auf Fehler (systematische gegenüber zufällig auftretender Fehler) ergänzen.

Sowohl das Produkt als auch die Prozesse sind auch bei der der Erarbeitung einer geeigneten neuen Sicherheitsarchitektur in dieser Arbeit im Blick zu halten, obwohl die meisten Anforderungen an die Prozesse erst bei konkreter Produktentstehung mit Entwicklung und Fertigung zum Tragen kommen. Das neue technische Konzept soll nämlich die normalerweise nur durch Prozess- und Methodenanforderungen erreichbare, systematische Sicherheitsintegrität durch seine Einfachheit und nach Möglichkeit auch durch das Konzept in sich unterstützen. Dennoch muss sich aber der Hauptteil der vorliegenden Arbeit um ein neues, technisches Sicherheitskonzept und bei der Betrachtung von Sicherheitsarchitektur und -mechanismen natürlich der Beherrschung von kritischen Fehlern im Betrieb zuwenden und wird sich weniger auf die Aspekte der Entwicklungsmethodik konzentrieren.

### 1.1.6 ÜBLICHE SICHERHEITSTECHNIK UND -MECHANISMEN

Zur Aufdeckung und Beherrschung von zufällig auftretenden Fehlern zur Betriebszeit von Elektronik bzw. ganzer ECUs bedarf es einer Architektur mit geeigneten Redundanzen und Sicherheitsmechanismen, beispielsweise zur Absicherung von Informationen[2], zum Vergleich von Daten oder zur Plausibilisierung von Zuständen. Beim Entwurf eines solchen Systems – technisches Sicherheitskonzept genannt– müssen sämtliche Möglichkeiten und Arten eines Ausfalls mit seinen potentiellen Auswirkungen betrachtet und mit der Definition entsprechender Maßnahmen und ausreichend schnell wirkender Mechanismen hinsichtlich Erhalt eines sicheren Gesamtzustandes berücksichtigt werden.
Maßstab und Stand der Technik in der Automobilindustrie für höchste funktionale Sicherheit von Steuergeräten ist heute noch immer das Sicherheitsgrundkonzept EGAS [22], bei dem auf vollständige Redundanz der sicherheitsrelevanten Signalwege verzichtet wird.
Es wurde ursprünglich für elektronische Motorsteuerungen entwickelt, über viele Jahre verfeinert und vielfältig eingesetzt. Noch heute gilt es in der Automobilindustrie als Referenzkonzept und das nicht nur für Aufgaben der Motorsteuerung.

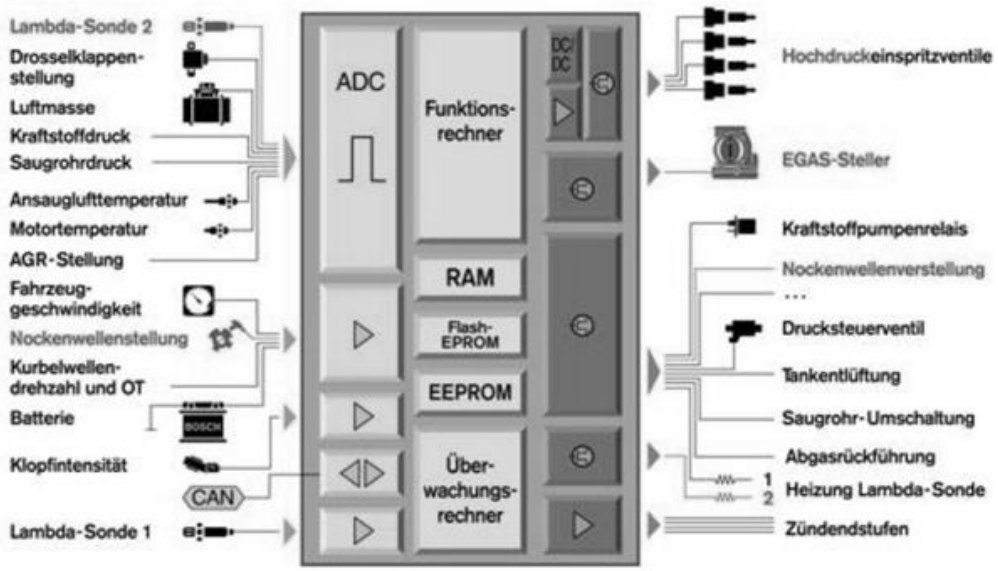



Abbildung 1.2: EGAS ECU (Bild: Robert Bosch GmbH)

Wie in Abbildung 1.2 ersichtlich, erfordert ein solches Sicherheitskonzept zum Beispiel zusätzliche Sensorik als Redundanz (links im Bild) und eine aufwändige Elektronik mit einer Einheit (mittig unten) zur Überwachung des Funktionsrechners (mittig oben).

[2] Information ist übertragbar; in Form von Daten bzw. Signalen. Digitale Information entsteht durch Digitalisierung beliebiger Information. Das Ergebnis sind Daten [66].

Die Fehlfunktion des Funktionsrechners muss als mögliche Gefahr betrachtet werden, die in irgendeiner Weise auch beherrscht werden muss. Der vorgesehene Sicherheitsmechanismus hierzu muss gefährliche Ausfälle einerseits rückwirkungsfrei diagnostizieren und das System andererseits im sicheren Zustand halten bzw., falls bereits ein gefährlicher Zustand eintrat, rechtzeitig in einen sicheren Zustand überführen. Das Konzept im Beispiel sieht zu diesem Zweck einen separaten Überwachungsrechner vor, der als Reaktion im Falle eines Fehlers im Funktionsrechner möglichst unabhängig von diesem Einfluss auf die Aktorik nehmen kann, zum Beispiel durch eine entsprechende Deaktivierung. In der Automobilindustrie galt und gilt in aller Regel der energiefreie Zustand und die Abschaltung der entsprechenden Funktionalität wie z.B. die Kraftstoffeinspritzung als sicher (Stichwort "fail safe", siehe Abschnitt 2.1.1). Ausnahmen bilden einzelne, aber moderat sicherheitsbezogene Funktionalitäten wie der Scheibenwischer oder das Abblendlicht, die im Bedarfsfall auch bei einzelnen Ausfällen der Technik operabel (Stichwort "fail operational", siehe ebenfalls Abschnitt 2.1.1) bleiben müssen.
Das oben dargestellte Konzept basiert noch auf diskreten Speicherbausteinen und einem separaten Mikroprozessor als Überwachungsrechner. Üblich ist heute ein einziges Rechnersystem mit einem integrierten Mikrocontroller (µC) und einer kleinen, diskret angeordneten Vergleichseinrichtung zu seiner Überwachung.

### 1.1.7 SICHERHEITSGERICHTETE ANWENDUNGEN

Sicherheitsgerichtete Anwendungen sind sicherheitsrelevante Anwendungen, die in besonderer Weise von ihrer funktionalen Sicherheit abhängen. Der Bezug einer Anwendung zur funktionalen Sicherheit ist durch viele einzelne Parameter definiert. SZs, Toleranzabstände, Anforderungsraten, mögliche sichere Zustände und das gesamte zeitliche Verhalten der Anwendung haben Bedeutung. Oft ist schon die Art und der Zweig der Industrie maßgebend: In der Avionik zum Beispiel ist die Abschaltung der Steuerenergiezufuhr kein möglicher sicherer Zustand, in den das System überführt werden muss, um im Falle des Versagens Gefährdungen abzuwenden. Trotzdem sind vielleicht die zulässigen Reaktionszeitintervalle beim Ausfall eines Ruders viel größer als sie bei Fahrzeugen üblich sind. Bei kleinen Kursabweichungen besteht zumindest nicht das unmittelbare Risiko der Kollision mit stehenden oder bewegten Objekten wie Brückenpfeilern oder Gegenverkehr wie auf der Straße. Die jeweils verwendeten Sicherheitskonzepte für aktuelle Systeme müssen also in Abhängigkeit von allen diesen Parametern angepasst sein und variieren daher mitunter sehr. Auch Kosten und die Stückzahl eines sicherheitsgerichteten Produkts spielen eine Rolle für die Wahl eines angemessenen Sicherheitskonzepts.

Im Straßenverkehr sind besonders kritische Anwendungen diejenigen, die Einfluss auf die Längs- und Querdynamik eines Fahrzeugs haben. Im Wesentlichen sind also besonders die Brems- und Lenksysteme betroffen.

Winkelsensorik im Automobil wird heute in aller Regel elektronisch unterstützt und spielt in den unterschiedlichsten Anwendungsfällen eine Rolle. Ob Pedal- und Drosselklappenstellungen, verschiedene Füllstände oder Hebelstellungen vermessen werden müssen, Winkelmessungen im Kraftfahrzeug sind zu alltäglichen, sehr oft sicherheitsbezogenen Aufgaben geworden.

Die aufkommende Elektromobilität und insbesondere der Trend zu elektronischen Fahrerassistenzsystemen verstärken den Bedarf an Drehwinkelsensoren, die dann im Gesamtverbund eines Fahrzeugs etliche Fahrzeugfunktionen gleichzeitig unterstützen müssen. Solche Funktionen können z.B. eine Geschwindigkeitsregelanlage (TMP[3]), ein Geschwindigkeitsbegrenzer (LIM[4]) und verschiedene Motorleistungssteuerungen sein, die alle gemeinsam auf einen Winkelmesser am Gaspedal angewiesen sind. Auch ein Lenkradwinkelsensor muss mit seinen Daten in der Regel eine Vielzahl von Funktionen im Fahrzeug bedienen, z.B. die Navigation, Scheinwerfer, die sich dem eingeschlagenen Kurs („Kurvenlicht") oder der Kulisse (AFL[5]) anpassen, die in den USA bereits obligatorische elektronische Stabilitätskontrolle (ESC[6]), die elektronisch gesteuerte, elektrische Lenkhilfe (EPS[7]), eine automatische Müdigkeitserkennung oder das geschwindigkeitsadaptive Lenken (AFS[8], ADS[9]).

Alle diese Funktionen unterliegen aufgrund der Serienfertigung in hohen Stückzahlen einerseits und dem breitgefächerten Markt andererseits einem enormen Qualitäts- und Kostendruck. Am Markt geforderte Funktionsvielfalt und -flexibilität zwingen die Hersteller zudem zu immer intensiverem Einsatz von Elektronik und Mikroelektronik mit SW. Dies alles stellt ein erhöhtes Sicherheitsrisiko dar, dem mit der strikten Umsetzung der standardisierten Anforderungen an die Sicherheitsintegrität und mit „intelligenten", d.h. möglichst einfachen Sicherheitskonzepten begegnet werden muss.

## 1.2 Zielsetzung und Beitrag dieser Arbeit

[3] Tempomat ™ Daimler AG
[4] Speed Limiter
[5] Adaptive Front Lighting, Adaptive Front Beam
[6] Electronic stability control, bei Daimler Benz AG und Volkswagen AG unter dem Namen *Elektronisches Stabilitätsprogramm* (ESP) bekannt.
[7] Electric power steering
[8] Adaptive Front Steering ™ Bayrische Motoren Werke AG
[9] Audi Dynamic Steering ™ Audi AG

Ziel und Beitrag ist ein in der Kombination von Mechanismen neues, möglichst einfaches, technisches Sicherheitskonzept zu entwerfen und dieses systematisch auf seine Eignung für höchste Funktionssicherheitsansprüche zu analysieren. Die sicherheitstechnische Güte, insbesondere die des wesentlichen Sicherheitsmechanismus (SM) in diesem für den Automobilbereich neuen Konzept, wird gründlich untersucht und anhand eines Diagnosedeckungsgrades (DC) kategorisiert, wie sie in den Sicherheitsnormen für bekannte SMs angegeben wird. Im Einsatz zur Lenkwinkelerfassung und -verarbeitung soll kanonisch und in Abgrenzung zu den im Automobilbereich üblichen Sicherheitskonzepten mit parallel redundanten Rechnersystemen für entsprechende, mechatronische Geräte, und insbesondere in Gegenüberstellung zum EGAS-Konzept als dem üblichen, an dieser Stelle verwendeten Sicherheitskonzept mit Ein-Rechner-System, gezeigt werden, ob, wie und unter welchen Umständen ein Automotive Safety Integrity Level D (ASIL D) nach ISO 26262 erreicht wird. Neben der Sicherheitsintegrität für die HW wird separat und explizit die systematische Integrität betrachtet, die per Konzept unterstützt durch eine vereinfachte Verifikation sichergestellt wird. Sämtliche, in Betracht kommenden Aspekte bezüglich Funktionssicherheit werden behandelt. Hinsichtlich Fehlertoleranzzeiten und sicherer Zustände werden Verbesserungen mit Möglichkeiten zu flexibler Funktionsdegradation und zu einem Notbetrieb gezeigt.
Die zu erörternden Fragen sind demnach:

- Wie kann durch ein möglichst einfaches, technisches Sicherheitskonzept höchste funktionale Sicherheit (ASIL D) erreicht werden?
- Kann dabei auf vollständige Redundanz oder zumindest auf die symmetrische Redundanz eines diskret aufgebauten Rechnersystems verzichtet werden?
- Werden sämtliche Einflussfaktoren zur funktionalen Sicherheit bezüglich zufälliger Ausfälle der Technik betrachtet?
- Wie kann Sicherheitsintegrität nachgewiesen, nachvollzogen und bestätigt werden?

Durch diversitäre Rückrechnung von Rechnerausgangsgrößen auf diversitäre Sensorgrößen wird trotz des nur einen, nicht redundanten Rechnersystems eine für ASIL D ausreichende Sicherheitsintegrität erreicht. Dazu dient eine in den zweiten, funktionell diversitär arbeitenden Sensorbaustein integrierte, und damit asymmetrisch angeordnete Vergleichseinrichtung (AAV). Im Falle eines durch diesen Sicherheitsmechanismus aufgedeckten Fehlers wird durch eine Ende-zu-Ende-abgesicherte Abschaltbotschaft für flexible Mög-

lichkeiten zur Funktionsdegradation und zu einem Systemnotlauf mit eingeschränkter Sicherheitsintegrität gesorgt.
Bei der Lösung werden folgende Teilbereiche abgedeckt:

- Prinzip und Vorteile der AAV
- Integration der AAV in Sensorbaustein und separierte Datenübertragung
- Übergänge in einen sicheren Zustand und Möglichkeiten zu Notlauf.
- Mögliche Fehler und ihre Beherrschung, HW- und systematische Integrität

Im Einsatz zur magnetbasierten Lenkwinkelerfassung wird konkret gezeigt, dass alle einzeln auftretenden, elektrotechnischen Ausfälle und auch systematische Fehler meist schon durch das Konzept bedingt sicher beherrscht werden. Auch mechanische Ausfälle und andere Fehlerquellen werden analysiert. Der Grad der erreichbaren HW- und systematischen Sicherheitsintegrität wird an den Kriterien der Norm ISO 26262 gemessen.

## 1.3 GLIEDERUNG

Die Arbeit ist in die drei großen Bereiche Voraussetzung, Stand der Technik und Lösungen und Ergebnisse gegliedert.

Abbildung 1.3 zeigt die Zuordnung der einzelnen Kapitel zu den Bereichen.

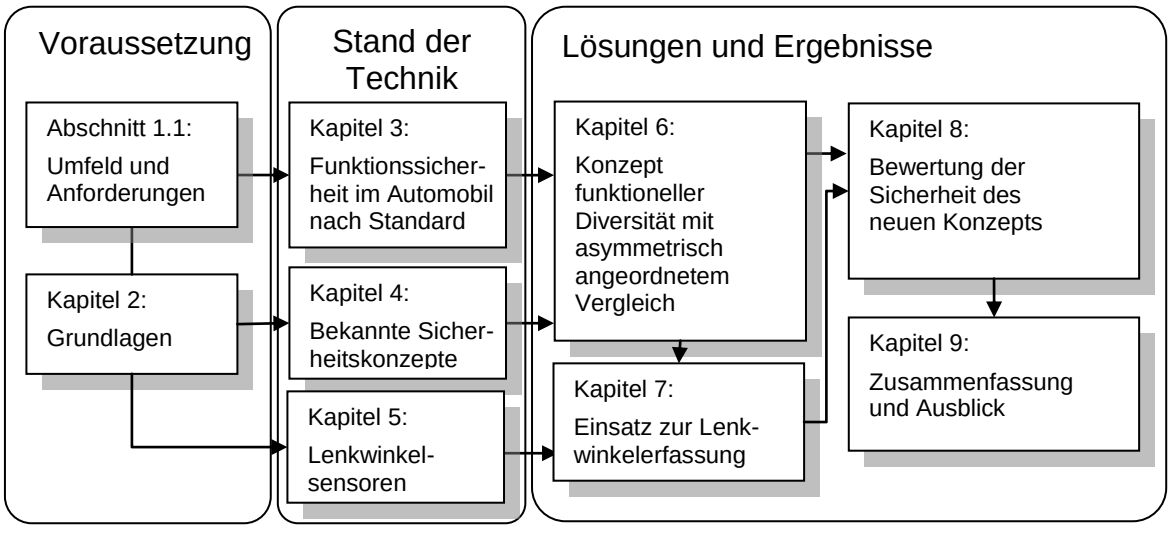



Abbildung 1.3: Gliederungsübersicht

Der Bereich *Voraussetzung* enthält mit dem Abschnitt 1.1 aus der Einleitung in Kapitel 1 das Umfeld mit seinen wesentlichen Anforderungen für die Ergebnisse der Arbeit. Kapitel 2 in diesem Bereich gibt einen Überblick über die allgemein sicherheitstechnischen Grundlagen, auf denen die Arbeit in den folgenden Kapiteln aufsetzt.
Im Bereich zum *Stand der Technik* sollen der Stand der Wissenschaft und Technik betrachtet und in Abgrenzung zu diesem sowohl konkretere Anforderungen als auch die Position der vorliegenden Arbeit definiert werden. Kapitel 3 darin enthält einen Überblick über die für den Automobilbereich geltende Norm ISO 26262 bezüglich funktionaler Sicherheit. Das ebenfalls in diesem Bereich enthaltene Kapitel 4 ist den bekannten Sicherheitskonzepten inklusive dem EGAS-Konzept zur späteren Gegenüberstellung gewidmet. Kapitel 5 stellt hingegen den aktuellen Stand der Technik für Lenkwinkelmesssysteme dar, an denen das neue Konzept später beispielhaft und konkret veranschaulicht werden soll. Hier werden die vielfältigen, harten Anforderungen an solche Systeme vertieft, mit der Praxis in der Automobilbranche verglichen und anschließend zusammengefasst, um daraus eine Vorgehensweise für ihre Erfüllung abzuleiten.
Die dann folgenden Kapitel stellen den Kern der Arbeit dar und werden in dem Bereich *Lösungen und Ergebnisse* zusammengefasst. Kapitel 6 enthält die Entwicklung, Ausarbeitung und Erörterung eines neuen, technischen Sicherheitskonzepts. In entsprechenden Unterabschnitten werden die verschiedenen Anforderungen an ein verbessertes Sicherheitskonzept, beispielsweise für einen Systemnotbetrieb, aufgegriffen und ein solches systematisch hergeleitet. Kapitel 7 beschäftigt sich mit der konkreten Anwendung des Konzepts für einen nach dem Noniusprinzip arbeitenden Lenkwinkelsensor. Die Ausführungen gehen dabei bis weit in den Entwurf von benötigter SW hinein. In Kapitel 8 wird eine ausgiebige Sicherheitsbewertung des ausgestalteten Konzepts vorgenommen. In entsprechenden Unterabschnitten geht es um Fehlerbeherrschung, mögliche Ausfälle der HW mit ihren Erkennungsmöglichkeiten, um den Umgang mit weiteren möglichen Fehlerquellen und um Möglichkeiten der Verifikation. Neben der steten Gegenüberstellung des Konzepts zu EGAS werden hier auch mögliche Variationen und Verbesserungen diskutiert. Abschließend werden besondere sicherheitstechnische Aspekte wie Fehlereinflüsse von außerhalb des Systems und durch die Mechanik beleuchtet. Die Arbeit schließt in Kapitel 9 mit der Zusammenfassung und einem Ausblick für zukünftige Verbesserungen und weitere Forschung.

# 2 SICHERHEITSTECHNISCHE GRUNDLAGEN

Dieses Kapitel enthält nun Grundlagen und einige Referenzen zur sicherheitsgerichteten Elektronikentwicklung, die zum Verständnis der Kapitel 6 und 8 benötigt werden. In die ISO 26262 wird separat in Kapitel 3 eingeführt. Auch die Grundlagen zum Stand der Technik bezüglich Sicherheitskonzepte und zu Lenkwinkelsensorsystemen finden sich gesondert (Kapitel 4 und 5).

## 2.1 FUNKTIONSSICHERHEIT

Sicherheit wird nach dem Stand der Technik mit der Freiheit von unvertretbarer Kombination aus Wahrscheinlichkeit und Ausmaß (Risiko) für Schäden an Menschen, Gütern oder Umwelt definiert. Ursächlich für solche Schäden sind Gefährdungen durch Situationen, Umstände oder Vorfälle.

Der Begriff »Sicherheit« ist in der deutschen Sprache ein Homonym[10], mit dem sowohl Angriffssicherheit und als auch Betriebssicherheit bezeichnet wird [13]. Während sich Betriebssicherheit (en: safety) auf den Schutz der Umgebung vor einer Sache bezieht, so betrifft Angriffssicherheit (en: security) den Schutz einer Sache vor Angriffen aus der Umgebung. Obwohl der Bereich Angriffssicherheit angesichts international organisierten Terrors ein immer wichtigeres Thema auch in Zusammenhang mit Betriebssicherheit ist und es auch schon bei der Normung Berücksichtigungsbestrebungen gibt (IT-Sicherheit integrierende Funktionssicherheit), soll dieser Bereich nicht weiter betrachtet werden.

Funktionssicherheit ist nun Teil der Gesamtsicherheit, der von der korrekten Funktion eines Systems und anderer risikomindernder Maßnahmen zur Abwendung von Gefahren abhängt.

Zur mathematischen Betrachtungsweise von Funktionssicherheit kann bereits [23] herangezogen werden. Gefahr und Sicherheit können demnach als komplementär zueinander betrachtet werden (Sicherheit =1 – Gefahr) [24].

Zur Definition aller in dieser Arbeit benutzten Begriffe sei grundsätzlich auf die Begriffs- und Abkürzungsdefinition der aktuellen Sicherheitsnormen [19] und [20] verwiesen.

### 2.1.1 GÜLTIGE NORMEN UND SICHERHEITSTECHNIK

Funktionssicherheit bedeutet Risikominimierung auf ein gesellschaftlich akzeptiertes Maß. Dieses Maß wird durch den durch Normen begründeten Stand der Technik definiert.

[10] Homonym bezeichnet ein Wort, das für verschiedene Begriffe oder unterschiedliche Einzeldinge steht. Homonym kann als Antonym (Gegenteil) zu Synonym betrachtet werden.

Der allgemeine Industriestandard für die Funktionssicherheit von Elektrik, Elektronik und programmierbarer Elektronik (E/E/PE) ist die seit 2003 erstmalig weltweit gültige Basisnorm IEC 61508, mit der alle anderen bisher geltenden Normen auch auf nationaler Ebene abgelöst wurden. Diese ist im Jahre 2010 in einer zweiten Edition [19] auf den heute gültigen Stand aktualisiert worden und wird als solche auch in für einzelne Zweige abgeleiteten Normen genannt, z.B. in der IEC 61511 für Prozessindustrie, in der ISO 25119 [25] für Land- und Forstwirtschaft oder in der ISO 26262 für Landfahrzeuge bis 3,5 Tonnen zulässiges Gesamtgewicht.

Der aktuell geltende Stand der Technik bezüglich Funktionssicherheit im Automobil ist der im September 2011 veröffentlichte Standard der ISO 26262 [20] in 9 Teilen. Ein weiterer Teil 10 (mit nur informativem Charakter) kam ab August 2012 geltend hinzu [26].

In allen diesen Normen wird im Allgemeinen mit steigendem Sicherheitsrisiko eine stufenweise Erhöhung der Sicherheitsintegrität definiert und gefordert. Nach ISO 26262 wird das Risiko und die entsprechende Sicherheitsintegrität in sogenannten *Automotive Safety Integrity Level* (ASIL) eingestuft. Die einzelnen Stufen werden im Allgemeinen einerseits durch einen sich verschärfenden, systematisch-methodischen Ansatz und zum anderen durch ein technisches Sicherheitskonzept und entsprechender HW voneinander abgegrenzt, die stufenweise engere Metriken bezüglich sicherheitsrelevanter Ausfälle der HW und ihrer Beherrschung einhalten müssen.

Die ISO26262 definiert als eine Stufe ohne besondere Sicherheitsintegritätsanforderungen das Qualitätsmanagement (QM) und darüber hinaus die Stufen ASIL A bis ASIL D für einfache bis höchste Sicherheitsintegritätsanforderungen. In der Norm, die übrigens zum Zwecke der internationalen Eindeutigkeit nur auf Englisch veröffentlicht wird, werden *Safety Items* von *Safety Elements* unterschieden. Eine Sensorkomponente wie ein Lenkradwinkelsensormodul stellt ein Safety Element im Rahmen verschiedener Safety Items dar, während ein Safety Item durch die Gesamtfunktion im Fahrzeug wie z.B. das ESP [27] definiert wird (vgl. ISO 26262 Teil 1). Die an einen Lenkradwinkelsensor gestellten SZs und Sicherheitsanforderungen mit ihren jeweilig zugeordneten ASILs ergeben sich demnach aus allen Gesamtfunktionen auf Fahrzeugebene, die den Lenkradwinkelsensor und seine Daten sicherheitsrelevant einbeziehen.

Eine Einzelkomponente als Safety Element im Verbund mit mehreren Safety Items im Fahrzeug muss dann die von allen SZs abgeleiteten Sicherheitsanforderungen mit dem jeweils höchsten ASIL erreichen. Die Gefahrenanalyse und Risikobeurteilung gemäß ISO 26262 haben in der Praxis beispielsweise für das „Safety Item“ *ESP* Sicherheitsanforde-

rungen mit ASIL B[11] für den Lenkradwinkelsensor ergeben. Typische Anforderungen einer EPS an einen Lenkradwinkelsensor können mit einem ASIL C als notwendige Sicherheitsintegrität behaftet sein und in die Lenkung eingreifende Systeme wie Aktivlenkungen oder gar rein elektrisch angesteuerte Lenksysteme (en: steer-by-wire) machen Lenkwinkelsensoren mit Anforderungen auf dem höchstmöglichen Niveau von ASIL D notwendig.
Die Funktionssicherheit bestimmter Systeme im Automobil, die wie das ESP-System z.B. einen Lenkwinkelsensor benötigen, wird durch Standards wie den *Federal Motor Vehicle Safety Standard* (FMVSS) oder die *Canadian Motor Vehicle Safety Regulations* (CMVSS) spezifiziert. Bei diesen produktspezifischen Normen geht es nicht mehr um Anforderungen an die Produktentstehungsprozesse, sondern vielmehr an das Produkt oder die Produktfunktion selbst. Dies können maximale Toleranzen, Zeiten oder ganz bestimmte, konkrete Mechanismen sein. Alle diese produktspezifischen Anforderungen zusammen mit dem allgemeinen Teil produktspezifischer Anforderungen aus der ISO 26262 für den Industriesektor umreißen die Sicherheitstechnik für eine Fahrzeugfunktionalität. Diese wird in einem logischen Konzept für Funktionssicherheit (en: Functional Safety Concept) für die Gesamtfunktionalität (Safety Item) und in den technischen Sicherheitskonzepten (en: Technical Safety Concept) für technisch separierbare Einheiten darin (Safety Elements) spezifiziert, beispielsweise für ECUs.
In diesem Zusammenhang ist von Bedeutung, ob und in welcher Weise das betreffende System durch Ausfälle eingeschränkt werden darf. Auch im Hinblick auf den nächsten Abschnitt zum sogenannten *Sicheren Zustand* sollen deshalb noch kurz drei Begriffe geklärt werden, die nicht in den bisher zitierten Standards erwähnt sind. Mit „**Fail Safe**“ wird das Verhalten einer Funktionseinheit oder auch einer einzelnen Funktion bezeichnet, wenn sie bei einem betrachteten Ausfall zwar ihre Funktion und Verfügbarkeit verliert, aber einen sicheren Zustand beibehält oder neu einnimmt. Ein plötzlich auftretender Stromausfall oder eine gezielte Abschaltung für eine Fahrerassistenzfunktion beispielsweise könnte einen solchen Zustand herbeiführen. Eine in dieser Weise schlichte Abschaltung des Prozesses oder der Funktion kommt für andere Anwendungen und Systeme nicht in Frage, wenn man z.B. an den Prozess des Fliegens mit einem Flugzeug denkt. Hier sind Systeme mit dem Ausfallverhalten „**Fail Operational**“ notwendig. Einzelne Ausfälle führen noch nicht dazu, Funktion und ausreichende Sicherheitsintegrität zu verlieren. Üblicherweise kann dieses Verhalten noch nicht mit einem einfach redundanten Systemkonzept erzielt werden, da der Ausfall in einem der beiden Kanäle durch beispielsweise einen

[11] Dies entspricht der Risikostufe eines schwachen SIL2 nach IEC61508. Die Anforderungen an die Sicherheitsintegrität für ASIL B sind dagegen deutlich höher als bei SIL2.

nachgeschalteten Vergleich zwar erkannt, jedoch nicht unbedingt lokalisiert und einem der Kanäle zugeordnet werden könnte. Gerade in Zusammenhang mit ADAS[12] oder dem automatisierten Fahren spielt dieses Ausfallverhalten natürlich eine immer wichtigere Rolle. Der dritte Begriff ist „**Fail silent**". Ein System verhält sich im Falle des betrachteten Ausfalls stumm. Daten werden weder gesendet noch empfangen und wie auch im Falle eines Stromausfalls reagiert es nicht weiter. Dieser Zustand muss noch nicht hinreichend einen sicheren Zustand bedeuten und es obliegt der technischen Peripherie im System, mit diesem Zustand in sicherer Weise umzugehen, um einen sicheren Zustand zu erhalten oder dorthin zu wechseln.

### 2.1.2 Der sichere Zustand und Abschaltpfade

Nach ISO 61508 [19] ist der sichere Zustand (en: safe state) der Zustand der EUC[13], wenn seine Sicherheit erreicht ist. Die ISO 26262 für den Kraftfahrzeugbereich ist hier etwas präziser: Ein Betriebsmodus des Systems ohne einen unvertretbar hohen Grad eines Risikos. Diese Definition geht weder von einem absoluten Zustand der Sicherheit aus noch knüpft sie diesen Zustand an einen vorherigen, potentiell gefährlichen Zustand. Im sicheren Zustand kann sich das System demnach auch im Regelbetrieb befinden, was natürlich und selbstverständlich erwartet wird. Von Interesse ist daher sowohl, wie der sichere Zustand eines Systems erhalten, als auch wie und in welchem Zeitintervall er im Falle eines Ausfallereignisses wieder erreicht werden kann. Beides ist gleichermaßen wichtig, setzt aber unterschiedliche Maßnahmen oder Mechanismen voraus. Zum Erhalt eines sicheren Betriebsmodus muss die Sicherheitsintegrität oder die jeweils verbleibende Integrität des Systems entsprechend hoch sein, was beim Entwurf beispielsweise durch Bauteilqualitäten oder den Einsatz von Redundanz und natürlich mit entsprechend hohem Anspruch an die Entwicklungsprozesse erreicht werden kann. Im anderen Fall, zum Erreichen eines sicheren Zustandes nach einem Fehler im Betrieb, müssen zunächst geeignete Mechanismen, d.h. zunächst Diagnosen in das System hinein entworfen worden sein, die einen potentiell gefährlichen Ausfall oder Fehler aufzudecken imstande sind.

Nach dem Erkennen eines kritischen Fehlers ist mit gleicher Sicherheitsintegrität auch eine Fehlerbehandlung und -beherrschung notwendig, mit denen der wie auch immer gestaltete Übergang zurück in einen sicheren Zustand möglich wird. Erkennen und Beherrschen von gefährlichen Fehlern gehört zusammen. Gute Fehlererkennung ohne Beherrschung oder Möglichkeiten der Fehlerbeherrschung ohne Aufdeckung sind sinnlos.

[12] ADAS – Automatic Driver Assistance System
[13] Equipment Under Control, gesteuerte oder geregelte Gerätschaften

Die meisten Systeme im Kraftfahrzeug können als sicher betrachtet werden, wenn sie energielos, d.h. elektrisch abgeschaltet sind. Schon im Konzept einer Funktionalität im Fahrzeug oder auch allgemein wird man darauf bedacht sein, diesen Zustand zu einem (endgültig) sicheren Zustand zu definieren. Möglichst wenige Systeme sollten für ihre Sicherheit auf elektrische Energie angewiesen sein, wie es beispielsweise für den Scheibenwischer oder ein Scheinwerferlicht bei Anforderung der Fall sein kann.
In der Regel geht es bei einem Sicherheitsmechanismus mit zugehöriger Fehlerbeherrschung also darum, das System gefahrlos und aktiv abschalten zu lassen, wenn sich der gefahrlose Zustand nicht durch die Art des Ausfalls schon von selbst ergibt, z.B. per Definition beim Ausfall einer Stromversorgung.
Für das aktive Abschalten der sicherheitsbezogenen Fahrzeugfunktion oder –funktionalität ergibt sich meist ein zusätzlicher Bauteileaufwand. Der gesamte Abschaltmechanismus, der wegen möglicher Bedingungsverkettungen, Schaltwege und Ansatzsorte auch oft Abschaltpfad genannt wird, kann sogar komplex werden, insbesondere dann, wenn zur Erreichung höherer Sicherheitsintegrität eine vom eigentlichen System unabhängige Abschaltung erforderlich ist. Alle zusätzlich herangezogenen Bauteile können natürlich auch selbst versagen, was sicherheitstechnisch ebenfalls betrachtet werden muss.
Beim Übergang von einem potentiell gefährlichen Zustand zum endgültig sicheren Zustand kann die ECU auch eine Anzahl von Sicherheitszwischenzuständen durchlaufen. Beispielsweise könnte ein Fehler nach seiner Erkennung zunächst zu einem gezielten Rücksetzen des eingesetzten Mikrocontrollers führen, sodann gezählt werden und erst nach wiederholtem Auftreten ein sukzessives Herunterfahren der Gesamtfunktionalität bewirken. Das System bzw. die Gesamtfunktionalität wird dabei schrittweise eingeschränkt, was eine Art **Degradation** darstellt. Für einige Situationen existiert ein sicherer Zustand nur so lange, wie die ECU einer kontinuierlichen Steuerung unterliegt. Diese kann temporär oder einen unbestimmten Zeitraum erfolgen.
Degradation ist zum Beispiel notwendig, wenn die betroffene Fahrzeugfunktion wenigstens eingeschränkt notwendig ist, das Fahrzeug gefahrlos anzuhalten. Der Begriff Degradation wird aber auch verwendet, wenn die betroffene Fahrzeugfunktion bereits im ersten Schritt komplett abgeschaltet wird oder ausgefallen ist und eine Weiterfahrt[14] mit sodann geringerer Sicherheit möglich bleibt. Üblicherweise wird der detektierte Ausfall technisch/elektronisch angezeigt und auf diese Weise dem Fahrer ein Teil der Sicherheitsverantwortung vom E/E/PE-System zurück übergeben.

[14] Engl. „limp home“ genannt, um das Erreichen des Fahrtziels oder einer Werkstatt zu ermöglichen.

Im Zusammenhang mit dem sicheren Zustand ohne Energiespeisung (fail silent/ fail safe, siehe vorheriger Abschnitt) hat der Begriff **Eigensicherheit** einer Schaltung eine besondere Bedeutung. Eine Schaltung, d.h. die Realisierung einer Funktionalität ohne den Gebrauch von SW, kann eigensicher entworfen werden. Kein einzelner Fehler in der Schaltung – gleich ob Unterbrechung, Kurzschluss, Potentialbrücke, Drift oder was auch immer – führt sie in einen gefährlichen Zustand. Allerdings ist die eigentliche Schaltungsfunktion nicht mehr unbedingt gewährleistet und verfügbar.

## 2.2 ZUVERLÄSSIGKEIT UND VERFÜGBARKEIT

Zuverlässigkeit (en: reliability) ist ein Begriff des Qualitätsmanagements. Nach [28] oder auch nach [29] ist Zuverlässigkeit die Fähigkeit eines Systems, während einer vorgegebenen Zeitdauer bei zulässigen Betriebsbedingungen ein funktionsgerechtes Verhalten zu erbringen, also korrekt zu arbeiten. Vorausgesetzt wird dabei ein technisches System, das keinen Entwurfsfehlern mehr unterliegt, sondern allein Umwelteinflüssen[15] ausgesetzt und, wie alles in der realen Welt, den Gesetzen der Physik unterworfen ist. Diese führen zu Alterung, Materialermüdung, Korrosion und ähnlichen Prozessen. Auch schon die Fertigungsprozesse mit Zuliefertransporten oder Zwischenlagerungen von Teilen unterliegen allerlei Umwelteinflüssen, die sich z.B. auf die Materialreinheit oder auf die Güte der einzelnen Komponenten auswirken.

Um sich der Bestimmung der Zuverlässigkeit eines Systems quantitativ zu nähern, bedarf es einiger stochastischer Grundlagen, die [30], [31] und [32] entnommen werden können.

Verfügbare Standards zur Zuverlässigkeit von Bauelementen sind werkseigene Normen wie Siemens SN27500 [33] oder besser international anerkannte Standards wie die IEC/TR 62380 [34], die IEC 61709 [35] oder amerikanische Normen wie die RIAC HDBK 217 Plus, die NPRD 95, die RIAC FMD97 und die MIL HDBK 338 [36]. Unter Anwendung dieser Standards werden üblicherweise mehr oder weniger pessimistisch gehaltene Basisausfallraten statt Zuverlässigkeitszahlen angegeben. Ausfallraten werden zur Vereinheitlichung und Vergleichbarkeit in FIT (en: failure in time) errechnet und angegeben. Ein FIT bedeutet $1x10^{-9}$ Ausfall pro Stunde oder anders ausgedrückt, statistisch ein einziger Ausfall nach einer Milliarden Stunden Betrieb.

Während die Zuverlässigkeit nun das Zeitintervall betrachtet, in dem eine Einheit korrekt funktioniert, bezieht sich Verfügbarkeit auf den zeitlichen Anteil, in welchem eine Einheit, eher in größeren Bauteilgruppen oder ein ganzes System, zur Benutzung bereit steht. Da-

[15] Physikalische Hardwareelemente sind beispielsweise durch Materialunreinheiten, Höhenstrahlung etc. untrennbar mit Ausfall- oder Fehlerwahrscheinlichkeiten verbunden.

bei werden auch die Reparaturzeiten berücksichtigt. Die momentane Verfügbarkeit ist definiert als die Wahrscheinlichkeit, eine Einheit zu einem vorgegebenen Zeitpunkt t der geforderten Anwendungsdauer unter vorgegebenen Arbeitsbedingungen in einem funktionsfähigen Zustand anzutreffen.

Im Gegensatz zur Zuverlässigkeit und Verfügbarkeit wird die systematische Eignung von Bauteilen nicht quantitativ angegeben, sondern wird über eine Qualifizierung sichergestellt. Diese kann im Bereich der Automobilzulieferindustrie für handelsübliche[16], elektronische Bauteile z.B. gemäß ISO 16750 oder über die Qualifizierungsstandards AEC Q100 für aktive oder AEC Q200 für passive erfolgen.

Die Zuverlässigkeit von Bauteilen sagt zunächst nichts darüber aus, ob oder wie sicher ein System arbeitet. In wie weit sich Ausfallstatistik sicherheitsrelevant auswirkt ist ohne eine spezielle Analyse der Anwendung noch keineswegs definiert. Entscheidend dafür ist eine Analyse der Ausfallarten und –effekte (FMEDA[17]), bei der geprüft wird, ob die untersuchten Bauteile je nach Ausfallart sicherheitsunkritisch ausfallen oder nicht. Wenn sie sicherheitsrelevant ausfallen, kann der kritische Anteil weiter reduziert werden, indem entsprechende Sicherheitsmechanismen, Diagnosen und/oder Fehlerbeherrschungen vorgesehen werden. Diese Sicherheitsmechanismen (en: safety mechanism, SM) tragen nichts zur eigentlichen Funktion des Systems bei. Sofern hierzu keine programmtechnischen Lösungen (SW, Software) zum Einsatz kommen können, erfordern diese Mechanismen meist zusätzliche Bauteile. Zusätzliche Bauteile aber machen ein System komplexer. Sie müssen natürlich wieder in Relation zu den Stückkosten des Gesamtsystems gesehen werden und können vor allem auch wieder versagen. Die über das technische System betrachtete Zuverlässigkeit nimmt durch den Einsatz zusätzlicher Komponenten ab, da die aufsummierten Ausfallraten größeren Anteil bekommen. In diesem Sinne steht Sicherheit der Zuverlässigkeit oder, genauer gesagt, der Verfügbarkeit kontraproduktiv entgegen. Im Extremfall sind die SMs derart komplex, dass ständig irgendeine zugehörige Komponente ausfällt und das System nie störungsfrei arbeiten kann und mehr repariert als genutzt wird. Auf eine sicherheitsgerichtete Fahrzeugfunktionalität bezogen wäre Sicherheit damit ad absurdum geführt. Ein Fahrzeug in der Werkstatt, in der Garage oder gar auf dem Schrottplatz wird am Ende völlig nutzlos, obwohl es dort als absolut sicher gelten muss.

Für den Normalfall kann jedoch von der idealen Vorstellung allgemeingültiger, absoluter Sicherheit unter Abwesenheit jeder Gefahr nicht ausgegangen werden. Für ein Sicherheitskonzept ergibt sich demnach immer die Frage nach der Verhältnismäßigkeit von Si-

[16] En: COTS – Commercial off the shelf im Gegensatz zu kundenspezifischen Bauteilen wie z.B. ASICs (application specific integrated circuit) oder FPGAs (field programmable gate array).
[17] FMEDA Fault Modes, Effekts and Diagnostics Analysis

cherheit in Bezug auf Komplexität und Aufwände, wobei die Einfachheit eines Konzepts immer der Sicherheit zuspielt und Aufwände nebenbei reduziert werden.

## 2.3 FEHLERARTEN UND -AUSWIRKUNGEN

Zur Definition der verschiedenen Fehlerarten und -möglichkeiten sowie zur ersten Analyse möglicher Fehler wird auf [37] verwiesen.

Abhängige Ausfälle (en: dependent failures) führen zu Fehlern, deren Wahrscheinlichkeit nicht als das einfache Produkt der Wahrscheinlichkeiten der individuellen Ereignisse, die den Ausfall verursachten, ausgedrückt werden kann [19]. Zwei Ereignisse sind nur dann abhängig, wenn gilt P(A und B) > P(A) x P(B). Zu abhängigen Fehlern führen zwei verschiedene Gruppen von Ausfällen: Kaskadierende Ausfälle (en: cascading failures) und Ausfälle infolge gemeinsamer Ursache (en: common cause failures, CCF) (siehe [20]).

Neben den systematischen Fehlern, die im nächsten Abschnitt kurz diskutiert werden, sind im Hinblick auf ein technisches Sicherheitskonzept vor allem zufällige Ausfälle von HW zu betrachten. Hierzu muss jedes einzelne Bauteil für sich analysiert werden.

Die Basisausfallrate z.B. eines Widerstands, aus Standards wie IEC/TR 62380[18] oder der IEC 61709[19] entnommen und um Betriebsparameter (z.B. Temperatur) angeglichen, muss zunächst auf die Ausfallformen verteilt werden. Eine angeglichene Basisausfallrate von vielleicht 5 FIT verteilt sich dann zu 3 FIT auf mögliche Unterbrechungen und 2 FIT auf mögliche Drift.

Ein wichtiger Schritt in der Sicherheitsanalyse, der üblicherweise nicht in den Beschreibungen des VDA für FMEAs auftaucht [38], ist nun die Analyse, ob sich die jeweilige Ausfallform sicherheitsrelevant bemerkbar macht, d.h. ob direkt oder indirekt mit Gefahren zu rechnen ist oder nicht. Ohne irgendwie verbundene Gefahren gilt der Anteil des Ausfalls mit der Rate $\lambda_S$ als sicher. Ausfälle, die eine Sicherheitsfunktion oder eines der SZs direkt verletzen würden, ohne durch einen Sicherheitsmechanismus (SM) oder eine Maßnahme beherrscht zu werden, werden nach ISO 26262 Einzelpunktfehler (en: single point fault, SPF) mit der Ausfallrate $\lambda_{SPF}$ genannt [20]. Trotz eingeplanter SMs muss mit einer Restfehlerrate $\lambda_{RF}$ aufgrund weiterer, gefährlich wirksamer Fehler (en: residual faults) gerechnet werden. Immer nur ein gewisser, im Übrigen zu begründender Prozentsatz der kritischen Ausfälle bzw. Ausfallformen können ausreichend beherrscht werden.

[18] Basis ist die französische UTE C80-811

[19] Basis ist die Siemens Werksnorm SN29500, sie ist jedoch speziell für den Bereich Straßenfahrzeuge ausgerichtet und bei den Fehlerraten etwa um Faktor 4 pessimistischer

Fehler, die die Sicherheitsfunktionen oder –ziele nur indirekt, also in Kombination mit einem oder mehreren anderen Ausfällen verletzen würden, werden nach ISO 26262 Mehrfachfehler (en: multi point faults, MPF) genannt. Sie führen zu Ausfällen mit der Rate $\lambda_{MPF}$. Im Rahmen der Sicherheitsanalyse[20] eines Bauteils zur weiteren Klassifikation ist nun notwendig zu unterscheiden, ob die betreffende Ausfallform latent, also unerkannt im System verbleibt (Rate $\lambda_{MPF,l}$), ob sie durch einen der eingeplanten SMs erkannt und beherrscht (Rate $\lambda_{MPF,det}$) oder ob sie sonst in irgendeiner Weise erkannt (en: perceived) und, wenn auch nicht technisch beherrscht, wenigstens beispielsweise durch ein Signal nach außen angezeigt wird (Rate $\lambda_{MPF,p}$).

Im Zusammenhang mit den zur Fehlerbeherrschung eingeplanten SMs ist es wichtig zu beachten, ob sie die Fehler innerhalb der kritischen Zeit beherrschen. So kann ein eingebauter Test (en: built-in self test, BIST) des Arbeitsspeichers (en: random access memory, RAM) beim Hochfahren des Systems sehr wohl zur Aufdeckung latenter Fehler dienen. Er wäre jedoch ungeeignet, um RAM-Fehler bei Systemen mit permanenter oder hoher Anforderungsrate unschädlich zu machen, wenn z.B. alle 100 Millisekunden eine sicherheitsbezogenen Funktion abläuft, die zum korrekten Ablauf unbedingt auf die Korrektheit des RAMs angewiesen ist. Hierbei ist unerheblich, ob das RAM an der betreffenden Stelle einmalig oder sporadisch, aber nur transient verfälschte Daten trägt oder ob es seit dem letzten Systemstart sogar irreversibel versehrt wurde.

Neben den induktiven Analysemethoden, ausgehend vom einzelnen Bauteil bis hin zur Auswirkung auf das Gesamtsystem sind deduktive Analysen bekannt, die also vom unerwünschten Ereignis auf Systemebene (en: top event) ausgehen und ihre Ursache sukzessive bis auf die einzelnen, beitragsleistenden Baugruppen und Bauteile herunter analysieren (en: top down). Bekannte Methoden sind z.B. die nach IEC 61025:2006 kurz FTA (en: fault tree analysis) genannte Zustandsbaumanalyse [39] oder auch die nach ISO 62502 kurz ETA (en: event tree analysis) genannten Techniken zur Analyse von Abhängigkeiten. Zu beachten für eine sicherheitsbezogene Analyse dieser Art ist natürlich, dass die zu untersuchenden Topereignisse nicht die unerwünschten Funktionsstopper sind, sondern eben die unerwünschten Verletzungen der Sicherheitsfunktion bzw. der SZs[21].

Nach ISO 26262 wird die Ausfallrate für die Verletzung eines SZs *Probabilistic Metric for Random Hardware Failures* (PMHF) genannt. Einheit für diese Metrik ist FIT ($10^{-9}$/h). Es geht hier wohlgemerkt zunächst „nur“ um die aus den einzelnen Ausfallraten hochge-

[20] Wegen der für Fehlerbeherrschung notwendigen Diagnose oft FMEDA genannt.

[21] Sicherheitsziele (en: safety goals) sind die Anforderungen an die Sicherheit des Systems auf höchster Ebene

rechnete Rate für zufällig eintretende Fehler mit Risikopotential, auch wenn die Systematik für CCF, d.h. die Art der vorgesehenen Redundanzen und sonstigen Zusatzmechanismen und -maßnahmen zur Gefahrenminderung mit berücksichtigt werden müssen.

## 2.4 Maßnahmen gegen systematische Fehler

In sicherheitsgerichteten Systemen stellt nach wie vor die Beherrschung systematischer Fehler die höchste Herausforderung dar. Im Entwicklungsprozess eines Systems sind hier natürlich die Bereiche Anforderungsmanagement, Konzept, Entwurf und Implementierung zu nennen. Werden die Anforderungen richtig kommuniziert, interpretiert und verfeinert? Wird die HW und vor allem die SW, sofern sie in sicherheitsgerichteten Systemen überhaupt zum Einsatz kommen soll, vollständig, korrekt und adäquat abgeleitet? Insbesondere der Entwurf und die Implementierung von SW stellt auch heute trotz aller verbesserter Methoden zur Unterstützung bei der Entwicklung ein großes Risiko für sicherheitsgerichtete Systeme und eine gewaltige Herausforderung bei der Fehlerbeherrschung dar. Man kann auch für weniger komplexe SW davon ausgehen, dass kein noch so umfangreicher Test sämtliche (systematisch verursachte) Fehler aufzudecken vermag. Auch der noch so systematische und gründliche Ansatz beim Entwurf und der Implementierung von SW strikt nach Phasenmodell und gegebenenfalls nach A-SPICE[22] [40] oder CMMI[23] [41] wird nicht alle Fehler ausschließen können. So muss für SW immer ein Restrisiko verbleiben und alle – auch in den entsprechenden Sicherheitsnormen genannten - systematischen Ansätze und Methoden bedeuten von daher immer nur eine entsprechende Risikominderung.

Darüber hinaus die vollständige Korrektheit eines Softwaresystems zu beweisen, sei es in einer mathematischen Darstellung, durch temporale Logik und/oder symbolische Analyse oder durch manuelle Verifizierung auf Maschinenbefehlsebene ist äußerst aufwändig und eigentlich nur bis zu einer gewissen Komplexität der SW mit vertretbarem Aufwand realisierbar.

Eine Rückübersetzung aller Maschinenbefehle (Assembler-Code) oder die Rückwärtsanalyse eines SW-Systems in die ursprüngliche Softwarespezifikation mit anschließendem Vergleich wäre ebenfalls noch ein gangbarer Weg zur Verifikation, der allerdings ebenfalls nicht uneingeschränkt zum Beweis der Korrektheit des Systems im Betrieb führt. Übersetzung und Rückübersetzung, auch wenn je von verschiedenen Teams oder Personen

[22] Automotive Software Process Improvement and Capability dEtermination, eine Adaption der ISO/IEC 15504 (SPICE) durch die AUTOSIG (en: Automotive Special Interest Group) von 2001

[23] Capability Maturity Modell Integration, herausgegeben vom Software Engineering Institute (SEI)

unternommen, unterliegt den systematischen Fehlern, die in bestimmter Kombination von Fehlern in beiden Richtungen als voneinander abhängige Fehler gemeinsamer Ursache Sicherheitslücken offen lassen. Gemeinsame Ursache wäre in diesem Fall beispielsweise eine bestimmte Art menschlicher Interpretation oder das zufällige und unerkannte „sich Aufheben“ der Fehler in beiden Übersetzungswegen. Trotzdem kann Rücktransformation als ein starkes Mittel zur Verifikation eines SW-Systems angesehen werden, da hier zwei möglichst unabhängige Seiten aus unterschiedlichen Blickwinkeln ein und dasselbe SZ verfolgen und die Wahrscheinlichkeit von kombinierten, sich kritisch auswirkenden Fehlern je nach Unabhängigkeit und Übersetzungsqualität vernachlässigbar oder zumindest vertretbar gering ausfallen wird. Bei der Rücktransformation könnte man im Gegensatz zu herkömmlichen Methoden zur Verifikation von einer Diversität sprechen. Begleitende Analysen, eventuelle Simulationen und vor allem verschiedenste Methoden des Tests auf allen Integrationsebenen eines Systems sind dennoch keinesfalls überflüssig und werden vom Stand der Technik gefordert.

## 2.5 Maßnahmen gegen zufällig auftretende Fehler

Standardmaßnahme gegen das Risiko spontan auftretender Ausfälle ist natürlich zunächst eine geeignete Bauteilauswahl. Höhere Festigkeiten, robustere Ausführungen, der Einsatz in Unterlast oder auch bessere Qualifikationen von Bauteilen sind definitiv dazu geeignet, sicherheitsrelevanten (wie auch für Sicherheit irrelevanten) Ausfällen vorzubeugen. In den vorangehenden Betrachtungen wurde aber schon deutlich, dass je nach geforderter Sicherheitsintegrität mehr unternommen werden muss.

Grundsätzlich ist auch an dieser Stelle Einfachheit oberstes Prinzip. Erst gar nicht verwendete Bauteile können auch nicht ausfallen, auch nicht sicherheitsrelevant. Eine klare Abgrenzung der sicherheitsrelevanten Teile von den unkritischen Teilen eines Systems oder Teilsystems mit möglichst einfachem, modularem Aufbau reduziert die Summe der sicherheitsbezogenen Ausfallraten. Wenn sich damit die Restfehlerrate ( $\sum(\lambda_{SPF} + \lambda_{RF})$ ) für eine sicherheitsgerichtete Funktionalität beispielsweise von 300 FIT auf 3 FIT reduzieren lässt, kann die Forderung der ISO 26262 nach maximal 10 FIT als Zielwert der PMHF für ein mit ASIL D eingestuftes SZ eines *Safety Items* schon erfüllt werden. Auch die Forderungen der ISO 26262 an die Metriken zur HW-Architektur (SPFM, LFM) lassen sich durch simplere Architektur leichter in den Griff bekommen. Der Aufwand für weitere, sonst notwendige Sicherheitsmaßnahmen und -mechanismen zur Erreichung der gleichen

Stufe an Sicherheitsintegrität[24] lässt sich durch Vereinfachung unter Umständen schon vermeiden.

Lässt sich nichts weiter zur grundsätzlichen Vermeidung von Ausfällen der sicherheitsgerichteten HW tun, müssen zur Erreichung der für eine bestimmte Sicherheitsintegrität genannten Metrikzielwerte die kritischen Ausfälle des Systems zur Laufzeit sicherheitstechnisch beherrscht werden. Dies kann auf unterschiedliche Weise erreicht werden. Grundsätzlich muss ein Fehler nicht notwendigerweise erkannt, diagnostiziert und aufgedeckt werden, um als beherrscht zu gelten. Beispielsweise die redundante, zweikanalige Ansteuerung (Highside / Lowside) eines Motors, der als definiertes SZ nicht ungewollt drehen soll, wäre eine durch das Konzept bereits gelöste Fehlerbeherrschung, ohne dass der Fehler in einer der Ansteuerungskanäle erkannt werden müsste, um das System in den sicheren Zustand zu führen. Eine fehlertolerante Architektur kann somit ohne Fehlererkennung auskommen, wenn die Hardwarefehlertoleranz (HFT, en: hardware fault tolerance[25]) für das System durchgängig im Hinblick auf den sicheren Zustand gilt. Andernfalls muss der Fehler an irgendeiner Stelle im System, vielleicht erst später in der Wirkkette und außerhalb der betrachteten Funktionseinheit, zur anschließenden Beherrschung erkannt, aufgedeckt oder diagnostiziert werden. Der Prozentsatz an Fehlern einer Ausfallkategorie eines Bauteils oder auch an Fehlern in größeren Zusammenhängen wird Diagnoseabdeckung (en: diagnostic coverage, DC) genannt.

Zur Diagnose und Beherrschung von Fehlern in Systemen ohne Fehlertoleranz dienen sogenannte Sicherheitsmechanismen (SMs), die zusätzlich eingeplant, entworfen, implementiert, eingebaut und verifiziert werden. Je nach geforderter Sicherheitsintegrität werden sich diese Mechanismen immer aufwändiger gestalten. Zu jedem vollständigen SM gehören, wie weiter oben schon erwähnt, eine Erkennung und eine Behandlung. Diagnose ohne entsprechende Reaktion, die den sicheren Zustand erhält oder einen neuen herbeiführt, ist wertlos. In diesem Sinne ist Diagnosedeckung selbstverständlich nur zurechenbar, wenn auch die entsprechende Reaktion betrachtet wird und die gleiche Sicherheitsintegrität wie die Diagnose besitzt.

Für verschiedene SMs ist es ebenfalls immer wichtig zu definieren, welche Ausfallarten erkannt und behandelt werden sollen. Liegen Fehler zugrunde, die mit einer gewissen Fehlertoleranzzeit direkt das SZ verletzen können (SPFs)? Oder sind es Ausfälle, die als MPF

[24] Für ein ASIL B wird beispielsweise eine SPFM von 90% gefordert, d.h., dass mindestens 90% möglicher Verletzungen eines Sicherheitsziels durch zufällige Ausfälle beherrscht werden müssen.

[25] Fähigkeit einer Funktionseinheit, eine geforderte Funktion bei Bestehen von Fehlern oder Abweichungen weiter auszuführen [19]. N+0 bedeutet, dass sich relevante Fehler ohne jede Toleranz gefährlich auswirken können.

bei Nichtbeherrschung nur indirekt Einfluss haben und latent im System verbleiben würden? Bei SPFs müssen in der Regel engere Zeitvorgaben[26] zur Erkennung und Beherrschung eingehalten werden als für die Erkennung und Behandlung von MPFs.

Als SMs kommen eingebaute Tests (z.B. initial oder zyklisch), Rücklesediagnosen, alle Arten von Redundanz mit anschließenden Vergleichen, Auswahlverfahren (Voter), Plausibilisierungen, aber z.B. auch Sicherheitsabfragen, Kontrollrechnungen, bestimmte Wertebereiche als Diagnosefunktion, Fangschaltungen oder Mechanismen (en: assertions) sowie sogenannte Überwachungseinrichtungen (en: watchdog, WD) in Frage. Als Maßnahmen und Verfahren zur Verbesserung der Hardwaresicherheitsintegrität werden verschiedene SMs für die unterschiedlichsten Schaltungsteile von Sensoren über Logik bis zu Aktoren in den Tabellen D.2 bis D.14 im informativen Anhang D des Teils 5 der ISO 26262 und in den Tabellen A2 bis A14 im normativen Anhang A des Teils 2 der IEC 61508 angeführt. In Anhang D der ISO 26262 in Teil 5 werden die genannten Mechanismen, zu denen übrigens in beiden Normen grob auch eine mögliche Diagnosedeckungsrate (hoch, mittel, niedrig) angegeben wird, erläutert.

Die Realisierung von SMs kann wahlweise in SW, in HW oder in einer Kombination dieser oder anderer Technologien vorgenommen werden. Die Flexibilität von SW und ihre Kosteneffizienz bei höheren Stückzahlen verleitet natürlich dazu, SMs ausschließlich in SW zu realisieren. Die Anforderungen für systematische Sicherheitsintegrität an SW, mit der solche SMs realisiert werden sollen, müssen von der SW, mit der die eigentliche Funktion realisiert werden soll, mehr oder weniger übernommen werden. Die Anforderungen an die Sicherheitsintegrität bezüglich zufälliger Hardwareausfälle gebieten natürlich auch bei der Realisierung eines SMs in SW, dass diese SW auf einer dem ASIL entsprechend unabhängigen HW abläuft bzw. selbst verschiedene HW zu ihrem Ablauf und zum Management des sicheren Zustandes nutzt. Eine mögliche Lösung könnte hier z.B. eine diversitär redundante Realisierung sein.

## 2.6 Redundanz und Diversität

Ziel von Fehlerbetrachtungen ist es, die Möglichkeiten, dass ein System wegen Eintreten eines oder mehrerer Fehler seine Funktion nicht korrekt ausführt, zu eliminieren und somit für Fehlertoleranz zu sorgen. Fehlertoleranz (en: fault tolerance) ist die Fähigkeit einer Funktionseinheit, eine geforderte Funktion bei Bestehen von Fehlern oder Abweichungen

[26] Zeitabschnitte des sog. Fehlertoleranzzeitintervals (FTTI) für jedes Sicherheitsziel

weiter auszuführen [19]. Andererseits ist auch dafür Sorge zu tragen, dass durch Fehlfunktionen kein Schaden entsteht und Sicherheit erhalten bleibt.

Im Bereich der Sicherheit wird Redundanz nicht zur Erhöhung der Verfügbarkeit, sondern zur Fehlerbeherrschung und zum Erhalt eines sicheren Zustands eingesetzt, um zum Beispiel durch bestimmte Sicherheitsarchitekturen[27] Fehlauslösungen zu minimieren.

Nach IEC 61508:2010 ist **Redundanz** (en: redundancy) zunächst das Vorhandensein von mehr als einem Mittel zum Ausführen einer geforderten Funktion oder zur Darstellung von Informationen. Beispielsweise wäre eine in Reihe geschaltete Sicherung redundant für den Fall, dass es bei einem Fehler auf eine Unterbrechung ankommt. Ein zweiter, parallel geschalteter Kondensator stellt eine Redundanz für die Funktion eines ersten Kondensators dar, wenn es auf den Erhalt einer Mindestkapazität ankommt und der Ausfall vorzugsweise eine Kontakttrennung ist. Ein drittes Beispiel, mehr zur redundanten Darstellung von Informationen, ist das Hinzufügen von Prüf- oder Paritätsbits.

Zur Kategorisierung von Redundanz wird nach [42] eine Gruppierung in Merkmale und Aktivierung vorgenommen. Die Merkmale von Redundanz lassen sich durch die Kriterien Struktur, Zeit, Information und Funktion charakterisieren. Zur Bezeichnung einer Redundanz wird bei technischen Systemen üblicherweise das Merkmal verwendet. Bezüglich Aktivierung geht es um den Zeitpunkt, zu dem redundante Mittel aktiviert werden. Im Zusammenhang mit Redundanz spielt zur Aufdeckung verschiedenartiger Fehler die Verschiedenartigkeit der eingesetzten Redundanzen eine wesentliche Rolle. Der Begriff für die Verschiedenheit von Redundanz ist **Diversität**. Nach IEC 61508 wird Diversität (en: diversity) durch ungleichartige Mittel zur Ausführung einer geforderten Funktion erreicht [19]. Diese können unterschiedliche physikalische Methoden oder unterschiedliche Lösungen für die gleiche Aufgabenstellung sein.

Die wichtigsten Diversitätsarten werden in [37], Seite 23ff und 116ff beschrieben. Die **Funktionelle Diversität** ist die zur Fehleraufdeckung hochwertigste Art der Diversität. Hier werden unterschiedliche Funktionen realisiert, deren Ergebnisse auf Erfüllung eines vorgegebenen Zusammenhangs hin geprüft werden (Plausibilitätsprüfung) [37]. Wie in Abbildung 2.1 zusammengefasst, lassen sich hier sogar weitere systematische Fehlerarten wie Konzept-, Spezifikations- und Entwurfsfehler entdecken.

In der Praxis kommen meist Mischformen der genannten Redundanzmittel zur Anwendung. Allein im Bereich des Entwurfs und der Implementierung von SW wird gezielt eine Vielzahl von Diversitätsformen, auch zur funktionellen Diversität, eingesetzt. An dieser Stelle sei zur weiteren Referenz das Vorlesungsskriptum Sicherheitsgerichtete Echtzeit-

[27] Eine Möglichkeit hier ist eine zweikanalige Struktur: 1oo2 (One out of two channel architecture)

system Teil I und II genannt [37]. Die folgende Abbildung darin kann als prinzipielle Richtschur gelten, auch wenn ihre Aussagekraft relativiert betrachtet werden sollte.

| Diversität | Erkennbarkeit von Fehlern | | | | |
|---|---|---|---|---|---|
| | Sporadische HW-Fehler | Statische HW-Fehler | Herstellungs-fehler | Implementa-tionsfehler | Funktions-fehler |
| der Einsatz-bedingungen | Ja | Nein | Nein | Nein | Nein |
| Physikalische | Ja | Ja | Nein | Nein | Nein |
| Herstellungs- | Ja | Ja | Ja | Nein | Nein |
| Implementations- | Ja | Ja | Ja | Ja | Nein |
| Funktionelle | Ja | Ja | Ja | Ja | Ja |

Abbildung 2.1: Diversitätsarten und Fehlererkennbarkeit nach [37]

## 2.7 FUNKTIONELLE DIVERSITÄT FÜR HOHE FUNKTIONALE SICHERHEIT

Auf die Stärke von funktioneller Diversität beim Einsatz von Redundanz wurde bereits in Abschnitt 2.6 hingewiesen. Mit funktioneller Diversität können verschiedenste Fehlerarten bis hin zu systematischen Fehlern aufgedeckt werden. Ein starkes Sicherheitskonzept für höchste Sicherheitsintegrität sollte daher auf jeden Fall den Einsatz von Redundanz mit funktioneller Diversität in Betracht ziehen. Eine Sicherheitsarchitektur mit diesen Konzeptelementen vermag die verschiedenen Ausfall-, Fehler- und Versagensarten im späteren Betrieb zur Laufzeit der realisierten Funktionalität aufzudecken, zu beherrschen bzw. sich zumindest ungefährlich auswirken zu lassen.

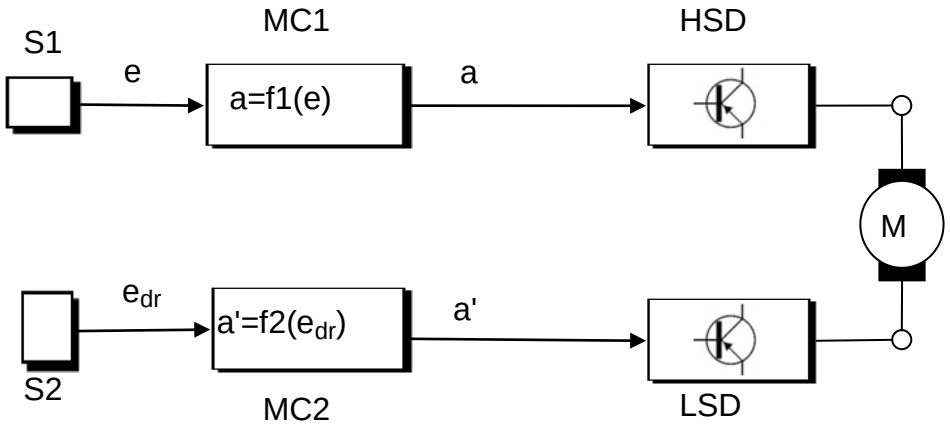
Normale systematische Fehler, beispielsweise in der Anforderungsanalyse, in einer Spezifikationsphase oder beim HW-Entwurf sollten in den üblichen Verifikations- und Validierungsphasen einer Produktentwicklung aufgedeckt und behoben werden können. An sämtliche systematischen Fehler eines SW-Systems (en: bugs) allerdings kommt eine im Automobilsektor übliche Verifikationsstrategie[28] nicht heran. Man muss davon ausgehen, dass eine komplexe SW immer Fehler beinhaltet. Unter Umständen machen sich diese erst sehr viel später zur Laufzeit, vielleicht in Kombination mit anderen Ausfällen, bemerkbar[29]. Dies bedeutet, dass es sich hinsichtlich systematischer Fehler lohnen kann, sich auch konzeptionell um ihre Beherrschung zur Laufzeit zu kümmern und entsprechende Möglichkeiten zu suchen und zu betrachten.

Es widerspricht der funktionellen Diversität in redundanten Signalpfaden ja nicht, in einem der Signalpfade auch eine SW oder ein SW-System einzusetzen. Sogar der Einsatz

[28] Diese umfasst in der Regel keinen mathematischen Beweis, keine vollumfängliche Zuteilbarkeitsanalyse oder dergleichen.

[29] Diese systematischen Fehler sehen daher oft wie zufällig aus und lassen irrtümlich Ausfälle der Hardware vermuten.

von zwei verschiedenen, diversitär entwickelten SW-Systemen in beiden Signalpfaden wäre denkbar. Abbildung 2.2 zeigt den schematischen Aufbau eines zweikanaligen Systems mit funktioneller Diversität ohne Vergleichseinrichtung.

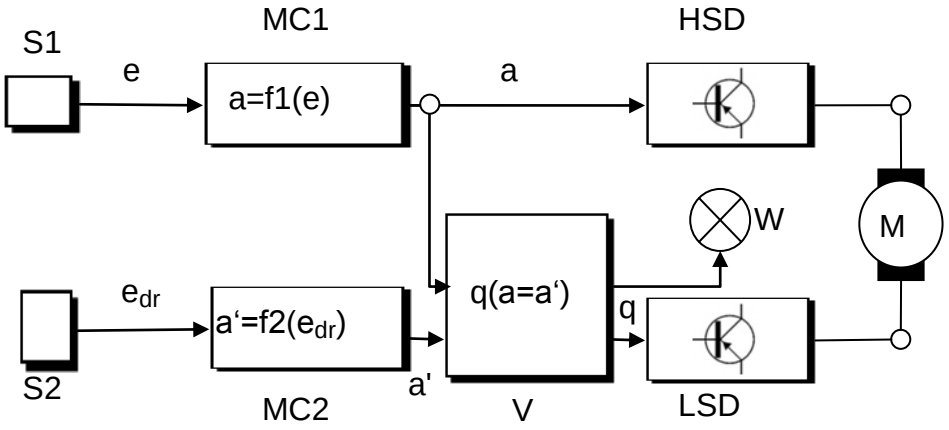



S1, S2: Sensoren mit funktionell diversitärer Redundanz und den Signalen e und $e_{dr}$
MC1, MC2: diversitäre Mikrocontroller mit den Ausgangssignalen a und a‘
M: Elektromotor als Aktor; HSD: High-Side-Treiber; LSD: Low-Side-Treiber
Abbildung 2.2: System mit funktionell diversitärer Redundanz ohne Vergleichseinrichtung

Mit dem dargestellten Konzeptentwurf können SPFs kategorisch ausgeschlossen werden. Voraussetzung hierfür ist das alleinige SZ, dass ungewollte Motorbewegung verhindert werden müssen und die Bedingungen, dass der LSD ausschließlich Masse zuschalten kann und der HSD ausschließlich positive Spannung. Jeder erste, auftretende Fehler hätte dann nicht das Potential, das SZ direkt zu verletzen, sondern muss als MPF behandelt werden, der ohne weitere SMs entweder ungefährlich oder gefährlich, jedoch latent im System verbliebe. Damit sich einzelne Fehler nicht gefährlich auswirken können, muss die funktionell diversitäre Redundanz, wie an anderer Stelle bereits erläutert, vollständig bis zum Aktor, beispielsweise bis zu einem Motor mit zwei Anschlüssen, durch das System gezogen werden.

Um erste MPFs bei solchem Konzeptentwurf im Betrieb tatsächlich aufzudecken und sie somit als $MPF_{RF}$s zu verhindern, bedarf es eines diagnostischen SMs. Hierzu könnte die Redundanz an einer möglichst fortgeschrittenen Stelle im Signalpfad ausgewertet und verglichen werden. Das Ergebnis des Vergleichs ist wiederum eine diversitär redundante Information, die einerseits angezeigt und mit der andererseits der redundante Pfad bis zum Aktor diversitär fortgeführt werden kann. In der Regel muss dieser letztlich sicher deaktiviert oder abgeschaltet werden, um mit dem System in einem sicheren Zustand zu bleiben. Die folgende Abbildung 2.3 verdeutlicht dieses Schema.

Es versteht sich von selbst, dass der Vergleich (und auch seine anschließende Fehlerbeherrschung) auf oder mit verschiedener HW laufen bzw. durchgeführt werden muss, um das Niveau der Hardwaresicherheitsintegrität zu halten, das durch die funktionell diversitäre Redundanz im Signalpfad einmal erreicht wurde.




S1, S2: Sensoren mit funktionell diversitärer Redundanz und den Signalen e und $e_{dr}$
MC1, MC2: diversitäre Mikrocontroller; W: Warnlampe; M: Elektromotor als Aktor
V: Vergleichseinrichtung; HSD: High-Side-Treiber; LSD: Low-Side-Treiber
Abbildung 2.3: System mit funktionell diversitärer Redundanz mit Vergleichseinrichtung und Warnlampe

Das Mittel hochwertigster, also funktioneller Diversität, verheißt also, nicht nur zufällige (gefahrbringende) Ausfälle der HW aufzudecken. Mit ihrer Hilfe und in geeignetem Umfeld können auch SW-Fehler beherrscht und per Vergleich sogar aufgedeckt und angezeigt werden.

Auch unter Einsatz von SW bleibt natürlich die Verschiedenheit und Unabhängigkeit der Vergleichs- und Fehlerbeherrschungs-HW von derjenigen Hardware wichtig, die den ununterbrochenen bzw. nicht per Vergleicher abschaltbaren Signalpfad bis zum Aktor bildet. Dieser direkte Signalpfad soll von hier an auch *Funktionspfad* genannt werden.

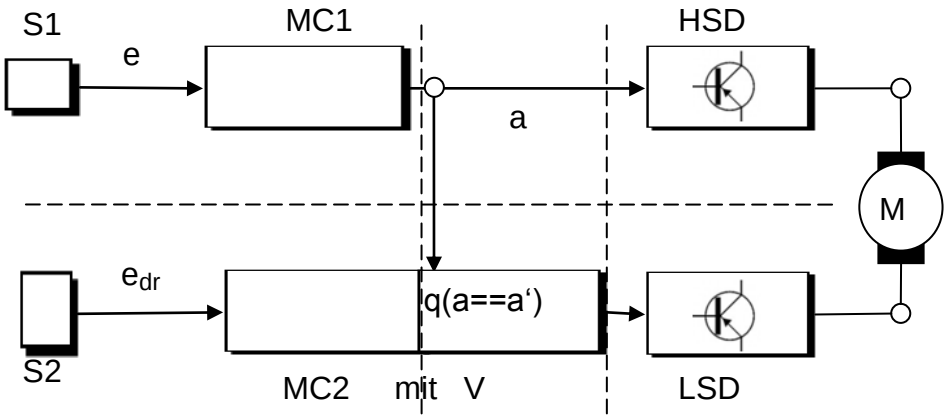
Die insgesamt erreichbare Sicherheitsintegrität setzt sich dann zusammen aus der des Funktionspfades und der des (dazu diversitären) Pfades mit SM.

Der SM besteht aus einer Vergleichseinrichtung V zur Fehlererkennung und -anzeige und dem Fehlerbeherrschungspfad zum Aktor hin, d.h. der Fehlerbehandlung hinsichtlich sicheren Zustands im Falle von nicht tolerierbaren Differenzen oder anderen Fehlern.

## 2.8 Verteilung der Auswertung funktioneller Diversität

Eine wichtige Voraussetzung zur Absicherung eines SW-Systems mittels redundanten Schutzsystems mit funktioneller Diversität ist zunächst seine Unabhängigkeit. Dies betrifft

in erster Linie seine Eigenschaften gegen mögliche Entwurfs- und Implementierungsfehler (Bugs) in der SW des abzusichernden Systemteils. Kein beliebiger Fehler der SW darf im diversitären Schutzsystem unerkannt bleiben, etwa durch identisch arbeitende Routinen. Idealerweise beinhalten der Zweig diversitärer Redundanz und das möglichst einfach zu haltende Schutzsystem erst gar keine eigene SW, da diese die Komplexität in der Regel deutlich erhöht. Das Schutzsystem darf keine einzige sicherheitsrelevante Routine des SW-Systems im abzusichernden Kanal beinhalten, sondern muss seine kritischen Vergleichsdaten bis zum abschließenden Vergleich und auch während der Fehlerbeherrschung funktionell verschieden halten und bearbeiten. Dies kann natürlich auch nicht mit derselben HW geschehen wie der im abzusichernden Kanal. Es ist also für das Schutzsystem wie in der Sicherheitstechnik üblich, ein eigenes, mit steigenden Sicherheitsansprüchen zunehmend diversitäres und damit zunehmend unabhängiger ausgelegtes Rechnersystem vorzusehen. Wie mit Abbildung 2.4 schematisch angedeutet kann die Vergleichseinrichtung V und das Rechnersystem MC2 im redundanten Signalpfad auch eine einzige, integrierte Schaltung sein. Dabei darf die für das neu entstandene Element geforderte Hardwaresicherheitsintegrität natürlich nicht für die verschiedenen Aufgaben und Bereiche unterschieden werden, sondern muss einheitlich über diese Einheit im sicherheitsrelevanten Signalweg gelten.




S1, S2: Sensoren mit funktionell diversitärer Redundanz und den Signalen e und $e_{dr}$
MC1, MC2: diversitäre Mikrocontroller; M: Elektromotor als Aktor; V: in MC2 integrierte Vergleichseinrichtung; HSD: High-Side-Treiber; LSD: Low-Side-Treiber; a: kodiertes Steuersignal
Abbildung 2.4: System mit integriertem Vergleich und symmetrischer Sicherheitsintegrität in zwei Kanälen

Abbildung 2.4 verdeutlicht die zwei durch eine gestrichelte, horizontale Linie getrennten, redundanten Kanäle eines Systems oben und unten. Die durch beide Kanäle zusammen erreichbare Sicherheitsintegrität basiert auf den Sicherheitsintegritäten jedes einzelnen Kanals. Die Integrität eines solchen Kanals ist durch die niedrigste Integrität eines Be-

reichs in der Reihe begrenzt, d.h. alle Elemente eines einfachen Signalwegs müssen mindestens die Integrität der für den Kanal angestrebten Integrität erreichen. Das schwächste Glied in der Reihe bildet sozusagen den Flaschenhals. Die für die beiden Kanäle jeweils erreichten Sicherheitsintegritäten dürfen aber unterschiedlich hoch sein, um in Kombination für das System insgesamt eine, wenn auch asymmetrisch verteilte, höhere Integrität zu erreichen. Die Gesamtsicherheitsintegrität setzt sich sozusagen aus den maximal erreichbaren Einzelintegritäten der parallel geführten Signalkanäle zusammen. Man könnte auch sagen, die angestrebte Gesamtintegrität muss auf die beiden, jeweils redundanten Zweige eines Signalwegs verteilt werden. Nach den Regeln möglicher ASIL-Dekomposition (s. Abschnitt 3.4.2) kann sich insgesamt ein ASIL B durch zwei Kanäle z.B. symmetrisch mit jeweils ASIL A(B) oder auch unterschiedlich verteilt mit einem Kanal bei vollem ASIL B(B) und dem anderen Kanal ohne ASIL (QM(B)) ergeben.

Die zwei gestrichelten, vertikalen Linien in Abbildung 2.4 trennen das System in drei Bereiche des Signalwegs. Der linke Bereich ist der Bereich einer symmetrisch redundant aufgebauten Sensorik. Der mittlere Bereich ist der Teil mit der redundanten Kontrolllogik samt Vergleichseinrichtung, die die beiden diversitär kodierten und vergleichbar gemachten Ausgangssignale miteinander plausibilisiert. Der dritte Bereich rechts ist wieder symmetrisch aufgebaut und führt die diversitäre Redundanz, nun in Form des kodierten Signals a oben und des vereinfachten Signals q unten, über die zwei verschiedenen Treiberstufen HSD und LSD zum Motor, dem Aktor des dargestellten Systems.

Für jeden unabhängigen dieser drei Redundanzbereiche muss die Zusammensetzung der Kanaleinzelintegritäten die angestrebte, kombinierte Integrität des Redundanzbereichs ergeben, um ein solches Konzept für die angestrebte Integrität des Systems konsistent zu halten. Dies bedeutet, dass die schwächste Kombination wieder den Flaschenhals bildet und die erreichbare Sicherheitsintegrität des Gesamtsystems begrenzt. Nach den Regeln für ASIL-Dekompositionen könnte man eine unabhängige Vergleichseinrichtung V im mittleren Bereich konform zu ASIL B(B) entwickeln und den oberen Kanalabschnitt, die Durchleitung des Signals, wie auch den gesamten oberen Kanal auf QM-Niveau belassen. Umgekehrt (nur die Durchleitung im mittleren Bereich oben auf ASIL B(B) und der Vergleicher unten auf QM(B)) macht es keinen Sinn, weil dadurch die Integrität des gesamten Systems das Niveau von QM nicht übertreffen könnte.

Die Aufteilung des Integritätsanspruchs auf die beiden jeweils parallel angeordneten Kanalabschnitte richtet sich nach Technologie, Komplexität und danach, wie wenig aufwändig für einen einzelnen Kanalabschnitt ein hohes Niveau an Sicherheitsintegrität erreicht werden kann. Beim Ansatz symmetrisch verteilter Integrität in die Redundanzkanäle ist es

folgerichtig, das Vergleichselement mit der Integrität eines einzelnen Kanals, also nach Dekompositionsanwendung, zu entwickeln und auszustatten. Die gilt erst recht für eine in ein anderes Redundanzelement hinein integrierte Vergleichseinrichtung. Für eine gemäß SZ des Items geforderte Integrität der Stufe ASIL D muss für die Integrität eines Redundanzkanals, samt oder ohne Vergleichseinrichtung, ein ASIL B(D) erreicht werden[30].

An dieser Stelle soll noch kurz der Einsatz zweier redundant eingesetzter Vergleichseinrichtungen in symmetrischer Konstellation betrachtet werden. In diesem Falle werden zwei verschiedenen Vergleichseinrichtungen beide redundanten Signale zum Vergleich zugeführt. Das SZ der Vermeidung eines ungewollt angesteuerten Aktors wird dadurch aber nicht besser erreicht. Außerdem kann im Fehlerfall die eigentliche Funktionalität, z.B. eine gewollte Aktivierung des Motors, wie bei der einfachen Vergleichseinrichtung auch nicht erhalten bleiben. Lediglich die Integrität der Vergleichseinrichtung selbst kann durch diesen redundanten Aufbau insgesamt erhöht werden. Die Vergleichseinrichtung wird durch den redundanten Aufbau natürlich aufwändiger und komplexer und ein Fehler darin statistisch wahrscheinlicher. Allerdings könnte der Ausfall einer Vergleichseinrichtung oder ein Fehler in einem der Vergleiche klar von Fehlern in der vorgeschalteten Sensorik unterschieden werden. Defekte Vergleichseinrichtungen könnten nämlich nach außen durch unterschiedliches Verhalten der zugehörigen Warnlampen angezeigt werden. Ein Fehler in der vorgeschalteten Sensorik hingegen würde sich durch eine einheitliche Warnanzeige bemerkbar machen.

Grundsätzlich sollte eine Vergleichseinrichtung, wie eigentlich auch der gesamte Schutzkanal mit verschiedenem oder sogar funktionell diversitär arbeitendem Rechnersystem, so einfach wie möglich gehalten werden, um damit eine für sich möglichst hohe und leicht zu erreichende Sicherheitsintegrität zu erhalten. Leider widersprechen sich manchmal die zur höheren Sicherheitsintegrität unumgänglich notwendige Redundanz und vor allem der Grad ihrer Diversität mit der generell zu suchenden Einfachheit. Die Findung geeigneter Kompromisse ist ein sehr weites Feld und fällt aus dem Rahmen dieser Arbeit. Das ganze Schutzsystem oder wenigstens die Vergleichseinrichtung wird jedenfalls auf das Nötigste reduziert. Möglichst weite Teile des Systems sollten durch funktionelle Diversität überdeckt und abgesichert werden. Der Idealfall ist eine leicht zu verifizierende Vergleichseinrichtung mit einem Abschaltmechanismus, der ohne Weiteres mit festverdrahteter HW realisierbar ist.

[30] Die Durchleitung eines Signals, z.B. von MC1 zum HSD, muss zum Erreichen von ASIL B(D) weiter abgesichert werden, z.B. durch eine Pulsweitenmodulation (PWM) des Signals. Nur so könnten die durch die Norm ISO 26262 empfohlenen Zielwerte der Hardwarearchitekturmetriken SPFM und LFM für diesen Bereich erreicht werden.

# 3 STANDARD DER FUNKTIONSSICHERHEIT IM AUTOMOBIL

Erst im November 2011 wurde die erste Ausgabe (1st Edition) der ISO 26262 für Funktionale Sicherheit für Personenkraftfahrzeuge bis 3,5 Tonnen maximal zulässigem Gesamtgewicht veröffentlicht. Bereits viele Jahre zuvor gab es Bemühungen in der Automobilindustrie, einen Standard mit dem Ziel zu definieren, ihn effektiv und effizient in die bestehende Prozesslandschaft zu integrieren [43].

Der Standard ISO 26262 spezifiziert einen Sicherheitslebenszyklus. Er definiert Methoden, Aktivitäten und Arbeitsprodukte (Dokumentation, Projektplanung, etc.), die während der Konzeptionierung und Entwicklung sowie während Produktion, Betrieb, Wartung und Entsorgung von sicherheitsbezogenen Systemen von Kraftfahrzeugen notwendig sind, um den durch den Standard gestellten Anforderungen nach funktionaler Sicherheit zu genügen. Die folgenden Abschnitte zu den Details der Norm und dem damit definierten Stand der Technik, insbesondere im letzten Abschnitt 3.4.2 zum Thema Dekomposition werden bewusst recht ausführlich erläutert. Erst vor diesem Hintergrund kann das neue Konzept, bei dem Redundanz, Diversität und auch die Beherrschung systematischer Fehler eine tragende Rolle spielen, nach dem geltenden Stand der Technik eingeordnet, verglichen und abschließend beurteilt werden.

## 3.1 GRUNDZÜGE DER NORM

Die ISO 26262 [20], [26] basiert auf der IEC 61508 [19] und spezifiziert die Anforderungen der Automobilindustrie über den gesamten Produktlebenszyklus. Wie kaum eine andere Sicherheitsnorm ist sie auf einen strukturierten Ansatz für alle Phasen der Produktentstehung fokussiert und orientiert sich für die Phasen der Entwicklung des Produkts an einem V-Modell [44]. Die normativen Teile (2 bis 9) enthalten verbal oder unter Zuhilfenahme von Tabellen formulierte Anforderungen zu Aktivitäten, Methoden, Aspekten und Bedingungen. Diese sind teils allgemeingültig, meistens jedoch entsprechend der geforderten Sicherheitsintegrität ASIL A bis D gestaffelt.

Naturgemäß sind die meisten der Normanforderungen Anforderungen, die die Arbeitsprozesse- und –weisen betreffen. Konkrete technische Anforderungen an das Produkt oder an Elemente davon kann die Norm nicht aufstellen. Sie liefert die HW betreffend je nach ASIL allerdings Anforderungen zur Erreichung bestimmter Zielwerte für verschiedene Sicherheitsmetriken. Auch werden allgemeine Hinweise und Anforderungen zur Zerlegung von Sicherheitsanforderungen (Dekomposition, siehe Abschnitt 3.4.2) in Teil 4 und

Teil 9 und zu technischen Maßnahmen in HW (Teil 5, Annex D) und in SW (Teil 6, Annex D) gegeben und spezifiziert.
Wichtig zu wissen ist außerdem, dass die meisten in der ISO 26262 nur einfach genannten Methoden und ihre Begrifflichkeiten in den informativen Teilen 4 bis 7 der Basisnorm IEC 61508 detailliert erläutert werden.

## 3.2 Herausforderungen der Norm

Hersteller und Zulieferer sind verpflichtet, den Nachweis liefern zu können, dass ihre Produkte den nach dem Stand der Technik geforderten Sicherheitsanforderungen entsprechen (Beweislast). Dieser Stand der Technik wird in der Automobilbranche durch die entsprechende Norm ISO 26262 umrissen, die ihrerseits das Minimum an notwendigen Empfehlungen darstellt. Konformität (en: compliance) zu diesem Standard bedeutet ein je nach Risikoklasse unabhängig bestätigter **Sicherheitsnachweis** (en: safety case). Ziel des Sicherheitsnachweises ist es, die sichere Funktion des vordefinierten Fahrzeugteilsystems zu begründen [45]. Es geht um nichts weniger als um die sicherheitstechnisch korrekte Funktion in ihrem gesamten Lebenszyklus und um deren klar definiertes Verhalten im Fehlerfall bezüglich sicherer Zustände und zeitlicher Abfolge. Hier spielen nicht nur die Erkennung und Beherrschung von Fehlern zur Laufzeit, beispielsweise durch den Einbau geeigneter SMs, eine Rolle, sondern vor allem die Maßnahmen zur Vermeidung oder frühen Entdeckung systematischer Fehler, also im Vorfeld eines möglichen Betriebs. Mit steigender Integritätsstufe werden neben einer anspruchsvollen Unternehmenssicherheitskultur eine Fülle von zunehmend formalen und systematischen Methoden und Maßnahmen für die verschiedenen Entwicklungsphasen und Ebenen gefordert.
Große Herausforderungen mit der Norm stellen sich auch bei der Wiederverwendung bereits etablierter und eingespielter Prozesse, Methoden und Werkzeuglandschaften. Wie können diese durch möglichst geringe Einwirkung bestehen bleiben und die für die Konformität zur Sicherheitsnorm notwendigen Schritte, Arbeitsergebnisse und Nachweise eingebracht oder ergänzt werden?
Ähnlich verhält es sich für die Wiederverwendung von vielleicht seit Jahrzehnten etablierten Fahrzeugsystemen. Diese und ihre Teilsysteme müssen hinsichtlich ihrer Konformität gegenüber der ISO 26262 überprüft und bei geringsten Änderungen sorgfältig auf dadurch eingebrachte Kritikalitäten analysiert[31] werden. Unter Umständen müssen nachträglich bestimmte Qualifikationen und Nachweise zur Betriebsbewährtheit (en: proven in use)

[31] durch sogenannte Einflussanalysen (en: impact analyses)

erbracht werden. Zu beachten und denkbar ist auch, dass eine seit Jahren im Einsatz befindliche Komponente oder Funktionalität heute vielleicht in einem anderen, sicherheitsbezogenen Kontext einzuordnen ist. Beispielsweise könnte ein Lenkwinkelsensor, der bislang gefahrlos in Zusammenhang mit einer Müdigkeitserkennung eingesetzt wurde, neuerdings für ein generell risikobehafteteres EPS oder gar für Steer-by-wire ( [46], [47]) eingeplant werden.

Eine weitere Herausforderung der Norm sind die in der Automobilindustrie üblichen, verteilten Entwicklungen. Eine sicherheitsgerichtete Gesamtfunktionalität, in der Sprachregelung der Norm „Item“ genannt, besteht in der Regel aus einer Vielzahl von mechanischen, elektrischen, elektronischen und/oder mechatronischen Komponenten, den nach Norm sogenannten „Elements“. Diese Elemente sind oft nicht nur untereinander, sondern auch mit Komponenten elektronisch vernetzt, die zu keinem (sicherheitsbezogenem) Item gehören. Zudem realisieren die vernetzten Komponenten häufig auch gleich mehrere Funktionalitäten, die zu unterschiedlichen Items und ihren SZs gehören und damit eventuell unterschiedlichen Risikoklassen angehören. Die einzelnen, für ein Item beauftragten Zulieferer und Hersteller müssen sowohl sicherheitstechnisch als auch bezüglich ihrer Arbeitsweise aufeinander abgestimmt werden.

Im Umfeld zunehmender, elektronischer Vernetzung der Funktionen im Kraftfahrzeug und in einem Geflecht unterschiedlichster Zulieferer liegt eine der größten Herausforderungen mit der Norm in einem „intelligenten Systementwurf“. Hier ergeben sich im Hinblick auf die effiziente Entwicklung kostengünstiger, sicherheitsbezogener Systeme allerdings auch große Chancen. Eine intelligente Verteilung von Sicherheitsfunktionen auf Steuergeräte, die zeitliche Limitierung des Systemeingriffs zur Steigerung der Kontrollierbarkeit [48] oder die Aktivierung von Airbags durch nebenläufige Teilsysteme [12] sind Beispiele für derartige Lösungen. Auch geschickt angewandte oder neu konzipierte SMs wie der im Kern dieser Arbeit beschriebene können bei dieser Herausforderung sehr nützlich sein.

## 3.3 Normative Entwicklungsmethodik

In diesem Abschnitt soll es um die Systematik in den Teilen 3 (Konzept), 4 (System) und 6 (SW) der Norm gehen. Unterabschnitt 3.3.1 ist um das Management (sicherheitsbezogener) Anforderungen konzentriert, während Abschnitt 3.3.2 die sicherheitsgerichtete Entwicklung von SW entsprechend der Norm beleuchtet. Auf weitere Aspekte von Teil 4 und auf den Teil 5 (HW) zur Entwicklungssystematik geht dann der nächste Abschnitt 3.4 ein.

In der Konzeptphase einer Produktentwicklung wird zunächst ein Item[32], eine möglicherweise sicherheitsbezogene Fahrzeugfunktionalität, definiert und klar abgegrenzt (Klausel 5 in Teil 3 der Norm). Es gilt sodann festzustellen, um welche Art Entwicklung es sich handeln wird, ob ein neues System zu entwickeln oder ob ein bestehendes System abgewandelt und ergänzt werden soll (Klausel 6 ebenda). In welcher Phase des Lebenszyklus muss mit dem neuen Projekt begonnen werden? Welche Phasen sind relevant und welche vielleicht nicht? Soll vielleicht kein ganzes System, sondern nur eine allgemein verwendbare Komponente entwickelt werden? Die Norm nennt solche Komponenten SEooC (en: Safety Element out of Context). Unter Umständen sind bestimmte Phasen, Teile oder Klauseln der Norm nicht relevant, z.B. Teil 5, wenn es um die Entwicklung einer Autosar Basis-SW[33] geht.

Sehr entscheidende Schritte sind dann die Gefahrenanalyse und die Risikobewertung (en: hazard analysis and risk assessment, HARA), durch die der Sicherheitsbezug überhaupt postuliert wird (Klausel 7). Unter Zuhilfenahme von Gefahren- und Situationskatalogen und dem informativen Annex B zur normierten Methode werden sogenannte Sicherheitsziele (SZ) definiert und diesen entsprechend ihrer Risiken eine der Sicherheitsintegritätsstufen ASIL A bis D zugeordnet.

### 3.3.1 SYSTEMENTWICKLUNG NACH NORM

SZs stellen die oberste Ebene der Sicherheitsanforderungen für ein Item dar, von denen im Folgenden die gesamte sicherheitsgerichtete Entwicklung ausgeht und alle verfeinerten Anforderungen abgeleitet werden. SZs können neben einem ASIL weitere Attribute haben. Von Interesse sind z.B. zeitliche Vorgaben und Toleranzen, physikalische Charakteristika und immer auch Fehlertoleranzzeiten sowie mögliche sichere Zustände.

Von den SZs werden zunächst funktionale Sicherheitsanforderungen abgeleitet. Die funktionalen Sicherheitsanforderungen werden auf Subsysteme, d.h. auf ECUs, Elemente, Komponenten oder auch externe Maßnahmen verteilt, sodass diese mit ihnen belegt werden und sich so ein sogenanntes Funktionales Sicherheitskonzept (FSK) ergibt (ISO 26262-3, Klausel 8). Das FSK ist ein Sicherheitskonzept aus rein funktionaler Sicht, eine logische Architektur und noch losgelöst von Technologie.

Mit der HARA, dem Ableiten von SZs und dem Herunterbrechen auf funktionale Sicherheitsanforderungen zum FSK hat die ISO 26262 bereits großen Einfluss auf die nachfol-

[32] Begriffsbestimmungen zu Item, Element, System etc. finden sich unter Abschnitt 3.4 zum Thema Sicherheitsarchitekturen

[33] AUTomotive Open System ARchitecture [79]

gende Entwicklung. Diese Phase der Konzeptionierung zeichnet sich bereits durch einen großen Entwurfsraum für die Möglichkeit vielfältiger Architekturentscheidungen aus.
Zu beachten und mit Hilfe begleitender Sicherheitsanalysen (siehe Teil 9 der Norm) zu spezifizieren sind bereits in der Konzeptphase neben den genannten Aspekten auch mögliche Redundanzen, Betriebsmodi, kritische Ausfälle, sichere Zwischenzustände sowie Möglichkeiten der Fehlervermeidung und -beherrschung. Fahrerwarnungen, Degradation, Notbetrieb, Entscheidungslogik und alle relevanten Zeitintervalle sind ebenfalls stets zu konzeptionieren bzw. klar und eindeutig zu definieren.
Funktionale Sicherheitsanforderungen und sicherheitsrelevante Konzeptelemente, die im Sinne der Norm Sicherheitselemente und zur E/E-Technologie gehören, erben den ASIL der SZs, von denen sie abgeleitet wurden. Derselbe ASIL wird mit der dann folgenden Ableitung von technischen Sicherheitsanforderungen an diese weiter vererbt. Ausnahmen hiervon ergeben sich bei sogenannter Dekomposition von Anforderungen (siehe Abschnitt 3.4.2), zum Beispiel bei Redundanz oder Fehlertoleranz. Auch für Anforderungen oder Elemente, die bei Versagen nicht direkt ein SZ verletzen (Behandlung von MPFs), können sich Ausnahmen für den ASIL als zugehöriges Attribut ergeben. Für alle diese Sonderfälle kann sich der geforderte ASIL entsprechend den Dekompositionsregeln nach Teil 9, Klausel 5 bzw. nach einer Regel in Teil 4, Klausel 6.4.4.4 reduzieren. Abschluss der Konzeptphase bilden Überlegungen zu Validierungskriterien. Sind alle Sicherheitsanforderungen bezogen auf das Item wirklich richtig? Wie und durch welche Kriterien können sie später weiter validiert werden?
Die ganze Struktur von zu behandelnden Sicherheitsanforderungen ist in Abbildung 3.1 dargestellt. Vom FSK ausgehend beschreibt Teil 4 der Norm die sicherheitsgerichtete Ableitung von technischen Sicherheitsanforderungen an einzelne, elektrische oder elektronische Teilsysteme, d.h. an Sicherheitselemente wie ECUs oder untergeordnete Elemente (Klausel 6). Prinzipiell gelten hierbei allgemein alle Regeln des Anforderungsmanagements (vgl. [49]).
Für jedes der Systeme soll mit den technischen Sicherheitsanforderungen im Rahmen des Systementwurfs ein Technisches Sicherheitskonzept (TSK) aufgestellt werden. Ein TSK ist ein Sicherheitskonzept aus technischer Sicht. Da sich jedes System aus Teilsystemen zusammensetzen kann, wird es für ein Item unter Umständen etliche TSKs geben.

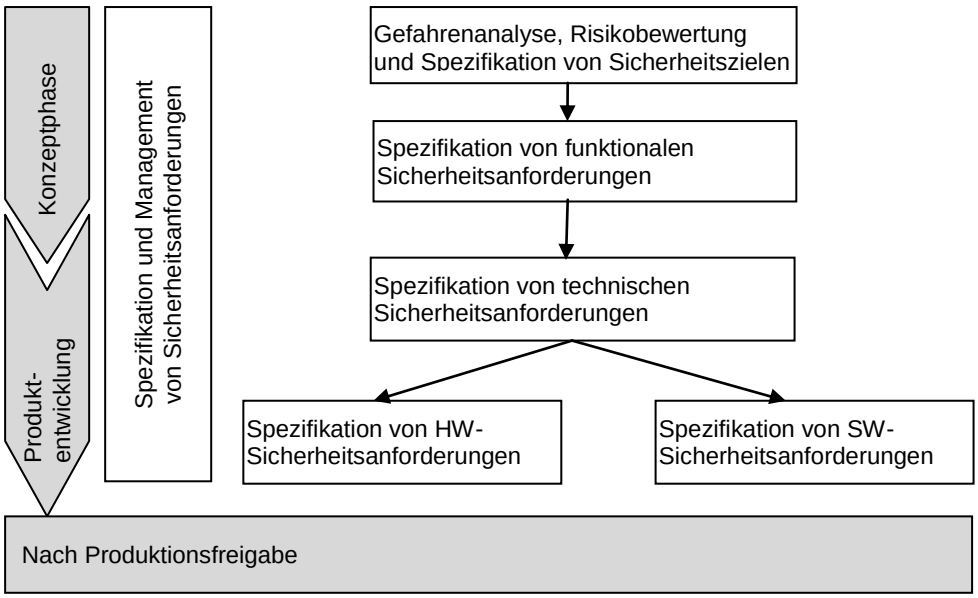



Abbildung 3.1: Struktur von Sicherheitsanforderungen

Wie in Teil 4 (Klausel 7) der Norm für das Systemdesign beschrieben, soll mit steigendem ASIL zunehmend Wert auf Modularität, adäquate Granularität und Einfachheit gelegt werden. Bekannten und altbewährten Prinzipien ist stets der Vorzug zu geben. Besonderes Augenmerk bezüglich Klarheit und Eindeutigkeit gilt den Schnittstellen, insbesondere zwischen in HW und SW geplanten Komponenten.

Ab höheren ASILs wird zur Unterstützung des Systemdesign neben der durchweg obligatorischen, induktiven Sicherheitsanalyse auch dringend eine deduktive Sicherheitsanalyse empfohlen. Diese Art der Analyse drängt sich in Entwürfen auf, in denen zur Erlangung höherer Sicherheitsintegrität verschiedene Redundanzen eingeplant werden müssen und der Entwickler einen Überblick über Unabhängigkeiten und mögliche CCFs benötigt. Zur entsprechenden Methodik wird auf Teil 9, Klausel 8 der Norm verwiesen.

Für die Verifikation von Anforderungen und des Entwurfs gilt das gleiche Prinzip. Für höhere ASILs reicht kein einfaches „Walkthrough“. Stattdessen soll zunehmend formal inspiziert, prototypisiert, analysiert, geprüft und simuliert werden.

Weiter wird in Teil 4 auch die Systemintegration und die Verifikation der Anforderungen behandelt (Klausel 8). Zu den einzelnen Integrationsphasen (HW/SW, Systemebene(n), Item, Fahrzeug) schreibt die Norm abhängig vom zugeordneten ASIL neben den naheliegenden Aktivitäten mehr oder minder strenge Methoden für notwendige Prüfungen, Testfallspezifikation und Umgebungen vor. Am Ende der Entwicklung des Items steht die Sicherheitsvalidierung.

### 3.3.2 Entwicklung von Software nach Norm

Die Entwicklung von SW im Rahmen von sicherheitsbezogenen Items (Teil 6 der Norm) unterscheidet sich nicht sonderlich von den herkömmlichen Phasenmodellen zur Softwareentwicklung (V-Modelle, SPICE [50]).

Zur Ableitung von Anforderungen gilt wieder allgemein Teil 8, Klausel 6 und zu ihrer Verifikation auf den einzelnen Abstraktions- und Integrationsebenen muss auf Klausel 9 in Teil 8 verwiesen werden. Sicherheitsgerichtetes Management der technischen Anforderungen verlangt unabhängig vom ASIL eine gut verständliche, eindeutige, atomare, testbare Spezifikation und bidirektionale Verknüpfungen (siehe auch Abbildung 8 der Norm in Teil 10) [26]. Mit zunehmend höheren ASILs werden die Ansprüche an die Entwicklungssystematik gesteigert. Dies betrifft z.B. den Gebrauch von defensiveren Implementierungstechniken, etablierten Entwurfsprinzipien, Entwurfsmustern mit entsprechenden Anleitungen und Richtlinien oder einer grafischen Entwurfsrepräsentation. Auch müssen Spezifikations-, Entwurfs- und Implementierungssprache zunehmend in ihren Stilmitteln eingeschränkt und vereinfacht werden. Ein zunehmend formaler Ansatz fängt bei festgelegter Syntax der Spezifikationen an und geht über eine definierte Semantik bis zu komplett modellbasierter Entwicklung mit möglicherweise automatischer Generierung von Quelltext. Der modellbasierten Entwicklung von SW ist ein eigener, informativer Anhang zu Teil 6 gewidmet (Annex B). Auf riskantere Konstrukte muss zunehmend verzichtet werden, wie zum Beispiel auf dynamisch erzeugte Objekte, Interrupts, umfangreiche oder allgemein offene Schnittstellen. Dagegen muss für höhere Integrität zunehmend auf engere Kohäsion, beschränktere Kopplung und auf Kapselung von Komponenten und Einheiten geachtet werden. Komplexität ist immer weitgehend zu vermeiden und durch geeignete Modularisierung und Strukturierung so weit wie möglich zu entflechten.

Außerdem müssen mit höheren ASILs zunehmend Mechanismen zur Absicherung und Verbesserung der Integrität entworfen und eingesetzt werden, beispielsweise Bereichsüberprüfungen von Eingangs- und Ausgangsdaten, Plausibilisierungen, externe Überwachungseinrichtungen, Kontrollflussüberwachung bis hin zu diversitären Parallelimplementierungen von Funktionen. Für die Implementierung gehören dieselben Prinzipien zum Standard, wie sie z.B. unter Einsatz der Sprache C mit dem Kodierungsstandard MISRA C [51] übereinstimmen.

Für die Integrations- und Testebenen schreibt Teil 6 wie auf Systemebene wieder je nach ASIL zunehmend striktere und umfassendere Methoden für die Erstellung der Testspezifikationen und die Prüfungen selbst vor. Testbereiche, -tiefen und -abdeckungen werden dem ASIL entsprechend weitgehender und systematischer gefordert. Auf unterster Verifi-

kationsebene werden Quelltexte manuell inspiziert und statisch analysiert, bevor sie den anforderungsbasierten Einheitentests (en: unit test) unterzogen werden. Mit SW-Integrationsprüfungen verschiedener Methodik sollen vor allem interne Schnittstellen zwischen Einheiten und Komponenten verifiziert werden. Weitere, möglichst werkzeuggestützte Analysen und Prüfungen sollen Laufzeitfehler finden, Freiheit von Beeinflussung und Störung (en: freedom from interference) (siehe auch Annex D und Teil 9, Klausel 6) und Robustheit nachweisen sowie die fehlerfreie Zuteilbarkeit von Zeit und anderen Ressourcen in der SW sicherstellen.

Besonderer Beachtung in Teil 6 der Norm gilt noch der normative Annex C, in dem es um die Herausforderungen von einerseits konfigurierbarer SW und andererseits von SW in Zusammenhang mit Kalibrierungen geht. Durch Konfigurationsmöglichkeiten kann schnell eine Unzahl schwer beherrschbarer Varianten entstehen, die sicherheitstechnisch natürlich grundsätzlich zu vermeiden sind. Die Komplexität von SW erhöht sich natürlich auch in Abhängigkeit von eingeplanten Kalibrierungsmöglichkeiten, die in der SW berücksichtigt werden und deren Verhaltensspielraum erheblich vergrößern und verkomplizieren.

## 3.4 SICHERHEITSARCHITEKTUREN

Zur Betrachtung von System- und Sicherheitsarchitekturen gemäß Norm müssen zunächst ein paar Begriffe und Bausteine erläutert werden.

Jedes System kann wiederum aus anderen (Teil-) Systemen bestehen. Einzeln oder unter Umständen auch zusammen bilden sie das sicherheitstechnisch abgegrenzte und zu betrachtende Item. Jedes (Teil-) System oder jede Komponente unterhalb eines Items wird Element genannt. Ein System kann z.B. als elektrisches/elektronisches System (E/E System), als Kommunikationseinrichtung oder als System anderer Technologie instanziiert werden (siehe auch Abbildung 4 in Teil 10 der ISO 26262).

Ein E/E-System wiederum kann beispielsweise ein elektronischer Sensor, ein Aktor oder eine Kontrolllogik (en: controller) sein. Jedes dieser Teilsysteme, z.B. ein Sensor-Steuergerät oder eine ECU, besteht aus verschiedensten Komponenten. Komponenten wiederum können aus HW, SW oder aus einer Kombination hieraus, vielleicht zusammen mit mechanischen Bauteilen wie Steckern, Gehäusen, Stellventilen oder Motoren bestehen (siehe auch Abbildung 3 in Teil 10 der ISO 26262). Eine HW-oder SW-Komponente aggregiert[34] sich aus einzelnen Bauteilen (en: HW part) oder SW-Einheiten (en: SW unit).

[34] d.h. setzt sich zusammen entsprechend der Nomenklatur der UML [80]

Komponenten lassen sich zuvor in weitere Komponenten einzelner HW-Blöcke und/oder SW-Module modularisieren, bis die unterste Ebene der Zusammensetzung erreicht ist.
Die Sicherheitsarchitektur für ein Item wird zunächst durch ein Sicherheitskonzept aus funktionaler Sicht (FSK) repräsentiert. Bei der Zerlegung dieses Konzepts in verschiedene Teilsysteme und Komponenten gilt die Aufmerksamkeit aus Sicherheitssicht primär den möglichen Verletzungen von SZs. Um die quantitativen Anforderungen und Zielwerte[35] für PMHF und SPFM (siehe dazu Abschnitt 3.4.1) zu erfüllen und später nachweisen zu können, sollten ab ASIL B bereits beim ersten Entwurf notwendige Redundanzen und Nebenläufigkeiten (Mehrkanaligkeit) für Datenerhebungen, Signalwege, Datenverarbeitungen und Ausgaben erwogen werden. Während für Konzepte mit maximal ASIL B annotierten SZs der Einsatz von Redundanz im Bereich der Sensorik (als Ort systembeherrschender Datenquellen) noch ausreichen mag, ist für Items auf Stufe ASIL D und Fail-Safe-Verhalten in der Regel schon eine durchgängige Redundanz von der Sensorik bis zur Aktorik notwendig.
Sensoren (und auch ihre Signalwege) sind dabei kritischer und prädestinierter für vollständige oder mitgeführte Redundanz, da ihre Ausgangswerte nicht wie bei der Aktorik z.B. zurückgelesen und plausibilisiert werden können.
Normgemäß soll jedes Element des Items mit dem zugehörigen ASIL gekennzeichnet werden. Für redundante Elemente kann sich der allozierte ASIL aufgrund von Dekomposition (siehe Abschnitt 3.4.2) verringern. Die für die Subsysteme vom FSK abgeleiteten TSKs als nächste Stufe des sicherheitsgerichteten Entwurfs sollten die Detaillierung der Sicherheitsarchitektur des Items für die einzelnen Elemente zur technischen Ansicht enthalten. Auch hier sollen redundante Elemente (bis zur Granularität von Komponenten) klar gekennzeichnet und mit dem zugehörigen ASIL (nach Anwendung der Dekompositionsregeln) versehen werden.
Für die Sicherheitsarchitektur auf technischer Ebene eines Elements kommen im Entwurf nun sekundär auch die Sicherheitsredundanzen und –mechanismen in Betracht, die gegen MPFs und latente Fehler eingesetzt werden sollen. Wie bei den Metriken PMHF und SPFM kann die Einhaltung der normativen Zielwerte[36] für die LFM natürlich erst später konkret[37] nachgewiesen werden. Deshalb verlangt das Konzipieren einer Sicherheitsarchitektur sehr viel vorausschauende Erfahrung. Falsche Entscheidungen können durch über-

[35] PMHF ab ASIL B: < 100 FIT, für ASIL D: < 10 FIT für ein Sicherheitsziel im gesamten Item;
SPFM für ASIL B: ≥ 90%, für ASIL C: ≥ 97%, für ASIL D: ≥ 99% für das jeweilige Sicherheitsziel.
[36] LFM für ASIL B: ≥ 60%, für ASIL C: ≥ 80%, für ASIL D: ≥ 90% bezogen auf ein Sicherheitsziel
[37] Nämlich erst dann, wenn der Entwurf der Hardware abgeschlossen ist und Schaltplan, Layout und Bauteilliste feststehen.

flüssigen Aufwand die Sicherheit verkomplizieren und nebenbei hohe Stückkosten verursachen. Wegen Verfehlung eines SZs könnten am Ende vorgegebene Entwicklungszeiten überschritten oder gar ein aufwändiges „Redesign“ der HW erforderlich werden.
In HW, SW oder in einer Kombination von Technologien realisierte Elemente bilden entweder einen Teil der eigentlichen, sicherheitsbezogenen Funktion (SF) oder in redundanter Weise dazu einen SM gegen SPFs oder gegen MPFs ab. Die Norm verlangt klare Kennzeichnungen und Eindeutigkeit bezüglich SF, SM, ASIL und anderer Attribute wie Fehlertoleranz (FT) und zugehörige Fehlertoleranzzeitintervalle (FTTI) bei SMs gegen SPFs. Für SMs, die zur Beherrschung von MPFs als sonst latente Fehler eingeplant werden, reduziert sich der zuzuweisende ASIL gemäß Teil 4, Klausel 6.4.4.4. Leider lässt sich durch die Syntax dieser Angabe nicht mehr auf den ASIL des maßgeblichen SZs schließen, wie dies bei ASIL-Angaben nach Dekompositionen durch die Klammern-Syntax noch eher möglich ist. Auch nach einer Kombination aus Dekomposition(en) und SM(s) gegen latente Fehler wird die Argumentation zur Reduzierung des ASIL unklar und sollte zur Sicherheit explizit dargelegt werden.

### 3.4.1 Entwicklung von Hardware nach Norm

Die Entwicklung von HW nach Teil 5 der Norm für sicherheitsbezogene Items verläuft ebenfalls phasenorientiert. Im Gegensatz zur Entwicklung von SW fällt für die HW die Empfehlung einer Verfeinerungs- und Integrationsebene im V-Modell weg (Teil 6, Klausel 8 und 9). Der Grund mag in der sehr oft höheren Komplexität und der Sicherheit ebenfalls entgegenwirkenden Flexibilität der SW-Technologie liegen. Stattdessen handelt Teil 5 in Klausel 8 und 9 von der Auswertung bzw. Bestimmung von Metriken zur HW-Architektur (en: single-point fault metric, SPFM; latent-fault metric, LFM) und zur Rate gefährlicher Restfehler (en: probabilistic metric for random hardware failures, PMHF).
Bei der Technologie *HW* haben wir es neben den systematischen Fehlern auch mit zufälligen Ausfällen zur Laufzeit zu tun, die man in ihrer Wahrscheinlichkeit quantitativ erfasst und denen gegebenenfalls durch die Art des Entwurfs und/oder durch SMs begegnet wird. Die Art des Entwurfs kann verschiedene Redundanz oder Eigensicherheit bedeuten. SMs können mit HW, SW oder einer Kombination der Technologien realisiert werden. Nicht nur deshalb wird in der Norm ein besonderer Schwerpunkt auf die Wechselwirkungen und Schnittstellen zwischen HW und SW gelegt, was sich unter anderem in der Forderung nach einer ausführlichen Schnittstellenbetrachtung (HSI) zwischen HW und SW als Arbeitsprodukt[38] bemerkbar macht.

[38] Hardware Software Interface Specification (HSI)

Zunächst verwunderlich scheint, dass in der Vorgabe der Norm die Phase der Verifikation der (Sicherheits-) Anforderungen an die HW (wie für SW in Teil 6, Klausel 11) fehlt. Dies mag daran liegen, dass zur Realisierung von Funktionen die HW eher die Plattform darstellt und die Funktionen eher in SW-Kategorien entworfen und realisiert werden.
Zur Ableitung von Anforderungen für HW gilt wieder Teil 8, Klausel 6. Auch bezüglich Verifikation der Anforderungen auf allen Abstraktions- und Integrationsebenen wird wieder auf Teil 8, Klausel 9 verwiesen (siehe auch Abbildung 7 in Teil 10 der Norm [26]).
Ferner gelten zu jeder Phase dieselben Prinzipien und Aspekte wie für die Ebenen von System und SW angesprochen. Mit zunehmend höheren ASILs werden die Ansprüche an die Entwicklungssystematik gesteigert. Ab SZs mit ASIL C soll für einen HW-Entwurf z.B. besonders auf Wartbarkeit, Diagnostizierbarkeit und Testbarkeit geachtet oder neben einer obligatorischen induktiven Sicherheitsanalyse auch eine deduktive Analyse durchgeführt und nachgewiesen werden.
Zusätzlich sollen zu allen Phasen der HW-Entwicklung die verschiedenen Arten zufälliger Ausfälle und ihrer zeitgerechten Beherrschbarkeit beachtet werden.
Bei der Verifikation kommen ab ASIL B z.B. Inspektionen (statt Review mittels Durchsicht), Sicherheitsanalysen nach Teil 9, Klausel 6 bis 8 (Beeinflussung, Koexistenz von Elementen, abhängige Fehler), Fehlereinstreuungstests und Prüfungen mit künstlicher Alterung hinzu. Ab ASIL C sollen statistische und erweiterte Funktionsprüfungen durchgeführt werden. Elektrische, chemische und normierte ESD/EMV Prüfungen sowie mechanische Festigkeits- und Dauertests sind für HW ungeachtet des ASILs obligatorisch.

### 3.4.2 DEKOMPOSITIONEN

In den Teilen 4, 5 und 6 der Norm zur Entwicklung von Systemen, HW und SW wird auf die Möglichkeit von Dekomposition nach Teil 9, Klausel 5 hingewiesen. Hierbei handelt es sich in erster Linie um die Zerlegung von Sicherheitsanforderungen aller Abstraktionsebenen von den SZs eines Items bis hin zu kleinsten Operationen oder Schaltvorgängen, die als Architekturelement in SW-Einheiten bzw. durch Bauteile realisiert werden können. Zweck dieser Zerlegungen ist eine dadurch gerechtfertigte Reduzierung der allozierten ASILs für daraus hervorgehende Anforderungen. Die Norm spricht deshalb auch von ASIL-Dekomposition. Natürlich gibt es dafür Regeln.
Als Grundregel erfordert die Anwendung von Dekomposition immer eine Form von Redundanz, die sich auf unterschiedliche und ausreichend unabhängige Elemente der Architektur bezieht. Eine Anforderung darf also nur dekomponiert und ihr zugewiesener ASIL reduziert werden, wenn die daraus für redundante und genügend unabhängige Elemente

abgeleiteten Spezifikationen dasselbe fordern[39]. Homogene Redundanz oder z.B. identische SW-Implementierungen (mit derselben Versions-/Revisionsnummer) sind generell ungeeignet.

Ausreichende Unabhängigkeit der redundanten Elemente kann und soll durch die Analyse von CCFs (en: common cause analysis, CCA) ermittelt und nachgewiesen werden. Unabhängigkeit ergibt sich umso mehr, je verschiedenartiger die eingesetzte Redundanz ist und je verschiedener die Elemente sind, durch die die dekomponierten Anforderungen realisiert werden sollen. Dabei sollte möglichst verschiedene Technologie und/oder verschiedene Prinzipien und Mechanismen erwogen werden (siehe Abschnitt 2.6 zu Diversität). Selbst die Entwicklung der Elemente durch unabhängige Personen oder Teams zur Aufdeckung von Entwurfsfehlern spielt eine Rolle in der CCA zu jeder Dekomposition.

Bei der ASIL-Dekomposition, insbesondere für SZs und Sicherheitsanforderungen aus funktional/logischer Sicht, muss nicht unbedingt ein anderes Element, z.B. ein E/E-System oder eine Komponente Träger der Realisierung sein. Auch rein mechanische Einrichtungen, andere Technologien oder gar Bedingungen außerhalb des Items dürfen zur Dekomposition herangezogen werden.

Wie früher bereits erwähnt, können den beiden aus der Dekomposition hervorgehenden Seiten auch unterschiedliche ASILs zukommen, was dann zu einer asymmetrisch verteilten Sicherheitsintegrität führt. In Abbildung 3.2 werden die diesbezüglichen Möglichkeiten bei einer Dekomposition dargestellt.

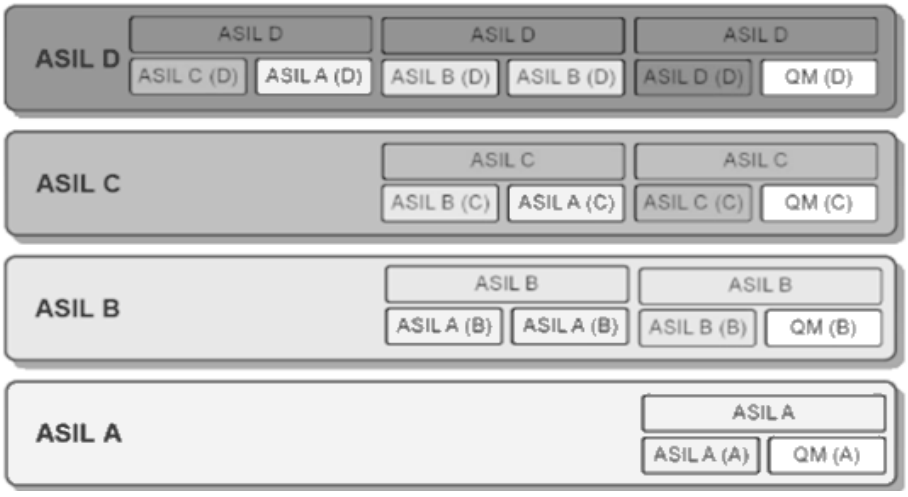



Abbildung 3.2: ASIL Dekompositionsschemen gemäß ISO 26262-9:2011

[39] Die ISO 26262-9 spricht in Klausel 5 - vielleicht etwas verwirrend - sogar von redundanten Anforderungen und Sicherheitsanforderungen,

In vier Ebenen wird darin jeweils links und in erster Zeile der ASIL des SZs angegeben, von dem die Dekomposition ausgeht. Die jeweils zweite Zeile gibt die Möglichkeiten der Zusammensetzung von dekomponierten ASILs an. Die zugrundeliegende Dekomposition wird bei der Angabe des ASILs durch die zusätzliche Angabe des ASILs des SZs in Klammern dokumentiert (z.B. ASIL B(D)).

Auch mehrfache Dekompositionen hintereinander sind möglich. In Klammern soll allerdings immer der ASIL des ursprünglichen SZs angegeben werden. Es fällt auf, dass ein ASIL A nicht durch Dekomposition aus nur QM-Elementen erreicht werden kann. Für ein SZ mit ASIL D werden nach kompletter Zerlegung mittels kaskadierter Dekomposition mindestens vier ASIL A(D)-Elemente benötigt. D.h. mit noch so vielen redundanten Elementen, die jeweils nur QM-Integrität erreichen, kann gemäß der Norm und durch Dekomposition kein höheres Integritätsniveau erreicht werden.

Die Norm schließt Dekompositionen in drei und mehr Pfade bzw. Elemente gleichzeitig nicht aus. Allerdings spielt der ASIL dritter oder weiterer, redundanter Elemente bei der Dekomposition normgemäß keine Rolle mehr zur Verbesserung des ASIL.

Bei der Verteilung der geforderten Sicherheitsintegrität bei ASIL-Dekomposition auf die jeweils zwei bei den Regeln herangezogenen Elemente sollte bedacht werden, dem einfacheren Element den höheren ASIL zuzuordnen.

Möglich und gebräuchlich sind auch ASIL Dekomposition zwischen der eigentlichen, sicherheitsbezogenen Funktion (en: safety of the intended functionality, SOTIF) und einem zugehörigen SM. Das Dekompositionsprinzip des höheren ASIL für das einfachere Element gilt insbesondere für Dekomposition von ASILs auf SMs, weil diese oft wesentlich einfacher aufgebaut sind als die eigentlich beabsichtigte Funktion, die damit abgesichert bzw. bei Ausfällen oder Fehlern beherrscht werden soll.

Die Dekomposition einer Sicherheitsanforderung mit ASIL D derart, dass der eigentlichen, die Anforderung realisierenden Funktion ein QM(D) zugewiesen wurde und dem entsprechenden SM ein ASIL D(D) zugeordnet werden muss, bedeutet dann, dass sowohl die systematische Sicherheitsintegrität als auch die Integrität der HW des geplanten SMs den entsprechenden Anforderungen der Norm (gemäß ASIL D) genügen muss. Im Falle eines solchen Mechanismus, der rein in SW realisiert werden soll, müssen neben der zu ASIL D passenden Entwicklungssystematik folglich zwei Aspekte beachtet werden. Einerseits muss die SW eine Integrität der Stufe ASIL D erreichen, was einen (weiteren) redundanten Ansatz notwendig machen kann, z.B. den Entwurf zweier diversitärer Verarbeitungs- und Fehlerbehandlungskanäle. Andererseits muss die HW, auf der dieser softwarebasierte SM laufen soll, nach wie vor eine Integrität von ASIL D (von D vor Dekom-

position) mit allen ihren Redundanz-Implikationen erreichen und außerdem noch gemäß den Dekompositionsregeln genügend unabhängig von der HW sein, mit der die eigentliche Funktion auf Stufe QM(D) realisiert wird.

Weitere Regeln und Bedingungen stellt die Klausel 5 in Teil 9 für ASIL-Dekompositionen auf. So sollen beispielsweise nach wie vor die Zielwerte der Sicherheitsmetriken für das gesamte Item gelten und erreicht werden. Die dekomponierten, technischen Anforderungen für zwei Elemente mit symmetrisch zugeordnetem ASIL B(D) sollen gemäß ASIL C spezifiziert und nachverfolgt werden.

# 4 BEKANNTE SICHERHEITSKONZEPTE

Sicherheitskonzepte werden aus Funktionssicht für ganze Sicherheits-Items (FSK) und aus technischer Sicht für Sicherheitselemente wie komplexe Sensormodule, Steuergeräte oder auch Einzelkomponenten aus HW oder SW (TSK) erstellt. In diesem Abschnitt sollen Prinzipien, Mechanismen und Konzepte betrachtet werden, die sich innerhalb von TSKs, beispielsweise für Lenkwinkelsensormodule (LWS), wiederfinden lassen.

In der Automobilindustrie gibt es seit über 20 Jahren das sogenannte EGAS[40]-Konzept für ECUs. Es handelt sich um ein stetig weiterentwickeltes TSK mit verschiedenen Prinzipien wie redundanten Ebenen, Überwachungsmechanismen wie einer Watchdog-Einrichtung oder anderen Mechanismen zum Übergang in sichere Zustände. Das Ziel aller Konzepte und Mechanismen ist es, die Sicherheitsintegrität der durch das Element realisierten Funktion insgesamt so zu verbessern, dass bei dessen Fehlverhalten bzw. Ausfall keine Gefährdung durch das Produkt entstehen kann (vgl. [52]). Die Prinzipien der Redundanz haben sich weiterentwickelt und werden in der ISO 26262 unter anderem als ASIL Dekomposition beschrieben [45]. Immer noch wird EGAS als Basis und Referenz aller TSKs für ECUs angesehen und für kritischste Sicherheitsaufgaben verwendet.

Redundanz muss nicht immer durch eine doppelt angelegte Zielfunktionalität (Sollfunktion) realisiert werden. Auch SMs, die unabhängig von der eigentlichen Funktion diese durch Zurücklesen von Informationen überwachen und kontrollieren, bieten Sicherheit durch etwas, was Redundanz genannt werden kann (siehe auch Abschnitt 3.4.2). Im Englischen, insbesondere im Flugzeugbau wird dann auch von einem Command/Monitoring-System gesprochen [45].

Meist wird versucht, diese Mechanismen unabhängig oder hinreichend rückwirkungsfrei in ausschließlich SW-Technologie zu realisieren, weil SW flexibler im Umgang ist. Für ausreichende Unabhängigkeit und/oder Rückwirkungsfreiheit sind aber zur Unterstützung oft auch weiterhin Maßnahmen auf System- oder HW-Ebene notwendig.

Es wird zudem grundsätzlich versucht HW-Komponenten-, Rechnersystem- oder Steuergeräteredundanz zu vermeiden. Diese Tendenz wird auch sehr stark von den Halbleiterherstellern unterstützt, die entsprechende Diagnose, Speicherseparierung oder Redundanz (diversitäre I/O-Peripherie, mehrere Rechnerkerne) auf einem Basischip anbieten [45].

Besondere Aufmerksamkeit bei der Erstellung eines Sicherheitskonzepts, das meist eine Kombination aus bekannten Konzepten und Mechanismen ist, verdient die angemessene

[40] Kurzbeschreibung unter [22]

Berücksichtigung der Fehlertoleranzzeitintervalle[41] (FTTI). Diese Intervalle, die bekanntlich in Bezug auf SPFs beachtet werden müssen, dürfen nicht unnötig eng definiert werden, da sich die Verfügbarkeit der Funktionalität im fertigen Produkt bei zu flink ausgelegter Fehlerreaktion, z.B. bei nur transienten Fehlerarten, schnell empfindlich herabsetzen kann. Ein dagegen zu lang angenommenes FTTI kann am Ende die notwendige Risikominderung verhindern, weil ein sicherer Zustand vielleicht nicht rechtzeitig eingenommen werden kann.

Zur Analyse und Beurteilung von Konzepten und ihrer erreichbaren Sicherheitsintegrität muss jeder einzelne Teilabschnitt im Pfad der sicherheitsbezogenen Informationen und Signale betrachtet werden. Für jede Station, für jeden Schritt im Signalpfad, muss mindestens die gleiche Sicherheit wie insgesamt für das betreffende Signal erreicht werden.

Mit Sicherheitsintegrität (der HW) ist in diesem Kapitel die Beherrschung von Fehlern durch zufällige Ausfälle gemeint, d.h. von SPFs unter Beachtung der FTTIs und von (sonst latenten) MPFs.

Auf einzelne, mit den wie folgt beschriebenen Sicherheitskonzepten kombinierbare SMs wurde bereits in Abschnitt 2.5 hingewiesen.

## 4.1 Redundante Sensorik

In elektronischen Sensoren als Quelle von Informationen und Messergebnissen werden digitale Daten und Messwerte erhoben. Jeder Messwert ist zunächst einzigartig, d.h. mit welcher Sicherheitsintegrität er erhoben wurde, kann er maximal weiter verwendet werden. Ohne Redundanz kann die erfasste Information mit nichts Vergleichbarem plausibilisiert und dadurch sicherer werden. Beim Konzept redundanter Sensorik geht es um den Einsatz irgend gearteter, möglichst diversitärer Redundanz. Diese kann zum Beispiel darin bestehen, neben dem elektrischen Taster zur Aufnahme eines Fahrerwunsches einen zweiten Taster mit invertierter Signallogik einzusetzen. Die Strategie dabei kann sein, so viele Daten mit vergleichbarem Informationsgehalt parallel zu erheben, wie in Abwägung zwischen Aufwand und Sicherheit gerechtfertigt erscheint. So kann sogar ein in sich redundanter Code entstehen, der für eine bestimmte Information steht. Bei einem Sensor mit optischem Wirkprinzip könnte dies der Gray-Code sein, der zum Beispiel bei der Abtastung eines Musters mit einer Kamerazeile[42] entsteht.

Gewisse Redundanz (siehe Abschnitt 2.6 zu Redundanz und Diversität) ist auch durch wiederholtes Einlesen möglich, wenn die zeitlichen Bedingungen und Toleranzen des SZs

[41] siehe Definition [20], Teil 1, Abschnitt 1.45 und Erläuterungen im Abschnitt 1.44

[42] Ein geeignetes elektronisches Bauteil zu diesem Zweck ist ein Array von Photo-Dioden (PDA).

dies erlauben. Die Abtastrate muss dabei natürlich erheblich höher sein als die Frequenz, mit der die Daten im Item zur Einhaltung des zugehörigen FTTI benötigt werden.

## 4.2 DAS KONZEPT 1OO1D MIT REDUNDANZAUSWERTUNG

*Ein Signal aus einem Kanal* oder kurz *Eins aus Einem* (en: one out of one, 1oo1) bedeutet, dass für den Weg eines Signals nur ein Quell- oder Übertragungskanal zur Verfügung steht. Zur Vermeidung von SPFs muss dieser korrekt arbeiten, d.h. die Eingangsdaten korrekt verarbeitet zum Ausgang bringen. Das „D" in der Bezeichnung 1oo1D steht für eine zusätzliche, interne oder extern nachgeschaltete Diagnose oder einen Diagnosekanal. Diagnose kann im einfachsten Fall eine Bereichsüberprüfung der behandelten Daten oder die Überwachung eines Spannungswertes sein. Selbstverständlich gehört zu solchen Diagnosemechanismen auch die nicht zu vergessende, angemessene Fehlerreaktion, und zwar noch innerhalb des notwendigen Zeitintervalls. Jedes D macht erst Sinn, wenn der aufgedeckte Fehler auch entsprechend beherrscht und ein sicherer Zustand eingenommen wird und erhalten bleibt. Erst dann ist der Begriff „Sicherheitsmechanismus" (SM) gerechtfertigt. SMs werden in diesen Konzepten eingesetzt, um Information in redundanter Weise abzusichern. Durch sie werden in erster Linie physikalische Ausfälle der HW, beispielsweise in RAM, ROM, CPU, Register, Halbleiterbauteilen und in allen anderen Bestandteilen beherrscht, d.h., das betrachtete Element wird in einem für das Item sicheren Zustand gehalten.

Als Unterstützung für die korrekte Verarbeitung von Daten und um bestimmte Diagnosen bzw. SMs überhaupt zu ermöglichen, müssen oft bestimmte Voraussetzungen geschaffen werden. Zum Beispiel könnten für die eigentlichen, informationstragenden Daten Wertebereiche definiert werden, für die sie ungültig sind, sogenannte Diagnosebereiche.

Der SM bei diesem Konzept kann aber auch darin bestehen, dass die Daten vor Eintritt in den einkanaligen Signalweg mit redundanten Daten ausgestattet werden, sodass die Gesamtheit dieser Daten am Ende oder außerhalb des Kanals miteinander plausibilisiert werden kann. Einfachste Beispiele für solche Mittel sind bei digitalen Daten ein Parity-Bit, eine Prüfsumme, ein CRC (en: cyclic redundancy code) oder gar eine auf Kryptografie basierende Signatur[43] in aufsteigender Reihenfolge ihrer Effektivität.

Analogdaten ohne Einplanung eines zweiten Kanals können z.B. durch eine Pulsweitenmodulation (PWM) kodiert oder differentiell übertragen werden. Bestimmte

[43] Eine kryptografische Signatur könnte z.B. ein auf RC4 basierender Hashcode sein.

Tastgrade bzw. Differenzen, in der Regel jedenfalls 0 und 100%, oder ganz gezielt ausgewählte Muster werden dann zur Fehlererkennung im SM herangezogen.
Wegen des fehlenden zweiten, vollständig redundanten Kanals kann in der Regel keine hohe Sicherheitsintegrität mit diesem Konzept erreicht werden. Durch nur partielle und unter Umständen unzureichend unabhängige Redundanz entstehen in der Absicherung oft Sicherheitslücken. Außerdem bedarf es zur Diagnose einer gewissen Auswerte- und Fehlerreaktionszeit, die sich bei der Beherrschung von SPFs ungünstig auf das zulässige FTTI auswirken kann.

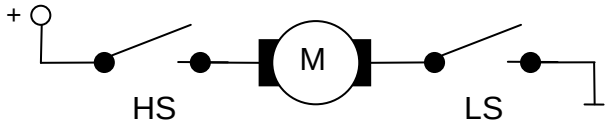
## 4.3 Plausibilisierung zurück gelesener Ausgaben

Zur Absicherung eines bestimmten Teilabschnitts im Signalpfad von Daten oder Befehlen wird gern das Konzept des Zurücklesens von Ausgaben gewählt. Einmal ausgegebene Daten oder Befehle werden dabei so weit wie möglich hinten im Signalpfad wieder aufgenommen, zurückgeführt und mit den ursprünglich ermittelten Ausgangsdaten verglichen. Beispiel hierfür ist das Zurücklesen von Botschaften auf dem CAN und der Vergleich des sicherheitsbezogenen Inhalts innerhalb der SW-Anwendung, um auf diese Weise sämtliche Fehler in der Signaletappe von der SW-Anwendung über die CAN-Treiberschichten in SW und HW aufzudecken und beherrschen zu können.
Ein anderes Beispiel, ebenfalls durch SW unterstützt, ist das Zurücklesen eines Wertes, der zuvor in den Speicher geschrieben wurde. Der abgedeckte Signalpfad ist hierbei ungleich kürzer, wird durch den Vergleich doch nur das korrekte Speichern, Schreiben und Lesen des betreffenden Wertes verifiziert.
Bei der Aktorik eines Items wird das hier beschriebene Konzept in größerem Stil eingesetzt. Auf den Einsatz redundanter Aktoren muss oft verzichtet werden, wenn es beispielsweise um aufwändige, bauraumintensive oder auch besonders teure Bauteile geht und ein Ausfall ohnehin den sicheren Zustand bedeutet (fail safe). Besonders gilt dies auch bei Bauteilen wie z.B. zwei redundant eingesetzten Elektromotoren, die im Fehlerfall gegeneinander wirken und dadurch das betreffende SZ und den sicheren Zustand technisch eher erschweren würden.
Direkt am Motor, beispielsweise einer elektrischen Parkbremse, einer elektrischen Lenksäulenverriegelung oder einer Lenkgetriebeverstellung werden deshalb die Potentiale der Anschlussleitungen abgegriffen, über eine AD-Wandlung im Steuergerät wieder eingelesen und mit den Sollwerten verglichen. Dies muss abhängig von den zugeordneten Fehlertoleranzzeiten natürlich zyklisch geschehen, wenn es um die Beherrschung möglicher

SPFs geht. Gegen latente Fehler im Fahrzeug dagegen reicht die Kontrolle oft einmal pro Fahrzyklus, beispielsweise bei der Initialisierung des Systems.
Bei einer redundanten Ansteuerung solcher Aktoren nach dem Konzept des nächsten Abschnitts 4.4 mit den zwei Anschlüssen *High-Side* und *Low-Side* geht es beim Mechanismus des Zurücklesens der Potentiale prinzipiell nur um die Beherrschung von MPFs zur Vermeidung von LFs.
Auch dieses Konzept ist zum Erreichen höherer Sicherheitsintegrität für ein Item allein nicht ausreichend. Es deckt sicherheitstechnisch wieder nur Teilbereiche ab und bedarf bestimmter Zeiten für die Diagnose und zur Absicherung der betreffenden Informationen.

## 4.4 DAS KONZEPT 1OO2(D)

Das Konzept 1oo2 (en: one out of two channels) stellt die Anwendung klassischer Redundanz dar. Durch die Realisierung zweier, symmetrisch angeordneter Signalpfade werden einzelne Ausfälle zunächst nicht durch einen SM mittels Diagnose beherrscht, sondern dadurch, dass ein sicherer Zustand schlicht erhalten bleibt. Bei der Ansteuerung eines Gleichstrommotors an beiden Anschlüssen, beispielsweise durch eine zweikanalige Brücke für High-Side und Low-Side wie im letzten Abschnitt angedeutet, bedeutet der Stillstand des (einen) Motors im Falle des Ausfalls[44] eines der (zwei) Ansteuerungskanäle, dass von ihm in Hinblick auf das SZ der Verhinderung ungewollter Motoraktivität keine Gefahr ausgeht. Abbildung 4.1 verdeutlicht die redundante Ansteuerung. Beide Kanalelemente links und rechts sind für ein solches SZ bei ausreichend Abstand zueinander auch hinreichend unabhängig.




HS: High-Side; LS: Low-Side; M: Gleichstrommotor
Abbildung 4.1: Zweikanalige Ansteuerung eines Motors

Anders sähe es aus, wenn der Motor an einer Seite fest mit einem der notwendigen Spannungspotentiale verbunden und die andere Seite mit beiden Zuschaltern in Reihe angeschlossen wäre. Ein einziger Fehler, ein Kurzschluss des Motoranschlusses mit dem anderen, den Motor aktivierenden Spannungspotential, würde das SZ verletzen.

[44] Unter Ausfall muss nicht unbedingt nur eine Unterbrechung, sondern kann wohlgemerkt z.B.auch ein Kurzschluss zu einem aktivierenden Potential verstanden werden.

1oo2-Konzepte werden auch in ECUs und besonders im Bereich der Sensorik eingesetzt, wenn es auf höchste Gesamtintegrität der Signale bzw. der Datenverarbeitung ankommt. Im großen Stil geschieht dies beim Einsatz ganzer Komponenten, d.h. verschiedener Sensoren oder Rechnersysteme. Standard ist dann z.B. der Einsatz zweier parallel rechnender Mikrocontroller. Im kleinen Stil könnten es zwei softwarebasierte Funktionen sein, die in diversitärer Weise zum intentionell gleichen Ausgabekommando (an verschiedenen Ports verschiedener Portgruppen) eines Mikrocontrollers kommen.

Geht es bei einem SZ um das Verhindern ungewollter Kraftwirkung oder Aktivierung, handelt es sich in der Regel um ein System, das beim Ausfall eines Signals[45], Befehls oder Wertes einen sicheren Zustand behält (fail safe), auch wenn bei Anforderung ebenfalls die eigentliche Funktion ausfällt. Diese Art Systeme, die beim beliebigen Abfall elektrischer Spannungspotentiale im System sicher bleiben, sind momentan die Regel für Automobile[46]. Mit autonom/automatisch geführten Fahrzeugen wird sich dies wohl ändern (vgl. [53], [54], [55] und *fail operational*). Jedenfalls können Einzelfehler in einem 1oo2-Konzept im Automobil bislang als sicher bezüglich direkter Verletzung der SZs angesehen werden. Erst ein zusätzlicher, sicherheitsrelevanter Fehler (MPF), der bei genügend Diversität der Kanäle sehr unwahrscheinlich gleichzeitig, d.h. im selben Fahrzyklus, im jeweils anderen Zweig auftritt, kann unmittelbar zu Gefahr führen. Zur Erkennung und Beherrschung dieser Fehler bedarf es zusätzlicher SMs oder Konzepte.

Bezeichnend für das reine 1oo2-Konzept ist, dass mit ihm kein Fehler lokalisiert[47] werden kann. Der den beiden Kanälen üblicherweise nachgeschaltete Vergleich vermag zwar den Fehler zu erkennen und vielleicht mit einem zusätzlichen Abschaltmechanismus zu begegnen, nicht aber den Fehler zu verorten. Beide Kanäle werden für die beabsichtigte Funktion unbrauchbar. Die Funktion oder die gesamte Funktionalität muss eingestellt werden und steht nicht mehr zur Verfügung. Zu Zwecken der Diagnose müssen für ein 1oo2D-Konzept und analog zu 1oo1D entsprechende Mechanismen bzw. ein Diagnosekanal eingesetzt werden.

## 4.5 Das Konzept N aus M Redundanz

In der Luft- und Raumfahrt oder auch anderen Industrien, z.B. der Atomkraftindustrie, ist seit Jahrzehnten das Konzept Triple Modular Redundant (TMR) bekannt. Hierbei wird

[45] Signale können neben ihrer Information auch Leistung übertragen.
[46] Ausnahme im Fahrzeug könnte beispielsweise die Scheibenwisch- oder –wascheinrichtung sein, die auf Anforderung funktionieren muss, um die Gefahr zu vermeiden.
[47] Fehlererkennung ist nur mit Hilfe zusätzlicher Konzepte oder Redundanzen möglich, z.B. durch die Auswertung von Kodierungen, durch Plausibilisierungen und andere diagnostische Maßnahmen.

dem 1oo2-Konzept ein weiterer Redundanzkanal hinzugefügt. Bei TMR geht es allerdings nicht um kleine und kleinste Abschnitte in den Signalpfaden, sondern um die parallele Steuerung und Regelung von Systemen durch ganze, unabhängige Module [56]. Diese haben beispielsweise ihre eigenen Gehäuse und Stromversorgungen. Im Fehlerfall darf – wie man sich vorstellen kann – der Prozess bzw. das Flugzeug (equipment under control, EUC) nicht ausfallen (fail operational), d.h. weder zwangsläufig, noch durch einfache Abschaltung.

In einem Noo3-Konzept ermöglicht der dritte Kanal einen Mehrheitsentscheid (en: voting). Der erste Fehler, der an irgendeiner Stelle im Konzept, d.h. in einem der drei Kanäle auftritt, kann im Hinblick auf die Übereinstimmung der anderen Kanäle klar lokalisiert werden. Wenn die Fehlerbeherrschung aus der Missachtung oder gezielten Abschaltung des fehlerhaften Kanals besteht, kann die Funktion mit zwei als valide angenommenen Kanälen fortgesetzt werden. Das als 2oo3-konzipierte System reduziert sich dann auf ein 1oo2-System. Ein dagegen als 1oo3-konzipiertes System setzt die Funktion nicht fort (schaltet komplett ab) und reduziert sich bis zur Reparatur auf das 1oo2-System. Zwischenzeitlich muss jeder weitere Fehler zum Stopp der beabsichtigen Funktionalität führen. Die Frage nach der angemessenen Zahl von Kanälen in einem N-aus-M-Konzept richtet sich demnach nach der Zeit[48], die bis zur Reparatur unter eingeschränkter Sicherheit vergehen darf.

Zur Anwendbarkeit dieses Konzepts im Automobil sollte außerdem und neben dem Aufwands- und Kostenaspekt Folgendes bedacht werden. Je mehr Kanäle eingeplant werden, desto unzuverlässiger (ohne Berücksichtigung der Sicherheit) muss das System wegen der Menge der benötigten Bauteile und ihrer Basisausfallraten werden. Alle Teile können ausfallen, über kurz oder lang Werkstattbesuche erfordern oder im Fahrzeug sogar den von Nutzern wie Herstellern gefürchteten "Liegenbleiber" verursachen.

## 4.6 DAS EGAS KONZEPT

Bereits vor über 2 Jahrzehnten wurde in der Automobilindustrie ein Sicherheitskonzept namens EGAS eingeführt. Ein entsprechendes Patent hierfür findet sich in DE4219457 [57]. Federführend war das Unternehmen Bosch AG mit diversen Zulieferern und OEMs wie Daimler-Benz AG. Anfangs ging es, wie der Name andeutet, noch um die sichere, elektronische Ansteuerung einer Drosselklappe[49], später um Motorsteuerungen allgemein. Zunächst betrachtetes SZ war aus gegebenem Anlass die Verhinderung des „Selbstbe-

[48] Diese Zeit wird statistisch gemittelt unter dem Begriff MTTR (en: mean time to repair) bezeichnet.
[49] Der Autor durfte im Rahmen seiner Tätigkeit als Entwickler bei VDO AG aktiv daran mitwirken.

schleunigers“. Wie mit z.B. der Autosar-Initiative und anderen Bestrebungen zur Standardisierung war es eine der Motivationen für EGAS, Anwendersoftware auf verschiedenen Systemen austauschbar zu machen. Das Konzept wurde im Laufe der Jahre immer weiter entwickelt, verbessert und auch für andere Anwendungen[50] angepasst. In der Automobilindustrie wurde das Thema Funktionssicherheit allerdings richtig systematisch erst mit der Entstehung der ISO 26262 angegangen. Bis dato war das VDA-Sicherheitskonzept EGAS, welches über die Jahre auch nach Japan und in die USA Verbreitung fand, das Basissicherheitskonzept in der Automobilindustrie (vgl. [45]). Charakteristisch für das Konzept ist stets die durch die Beschränkung auf ein einzelnes, nicht redundantes Rechnersystem begründete Einfachheit geblieben. Zuletzt wurde EGAS im Jahre 2006 von einem Arbeitskreis um verschiedene deutsche OEMs behandelt [58]. Abbildung 4.2 zeigt den prinzipiellen Aufbau darin.

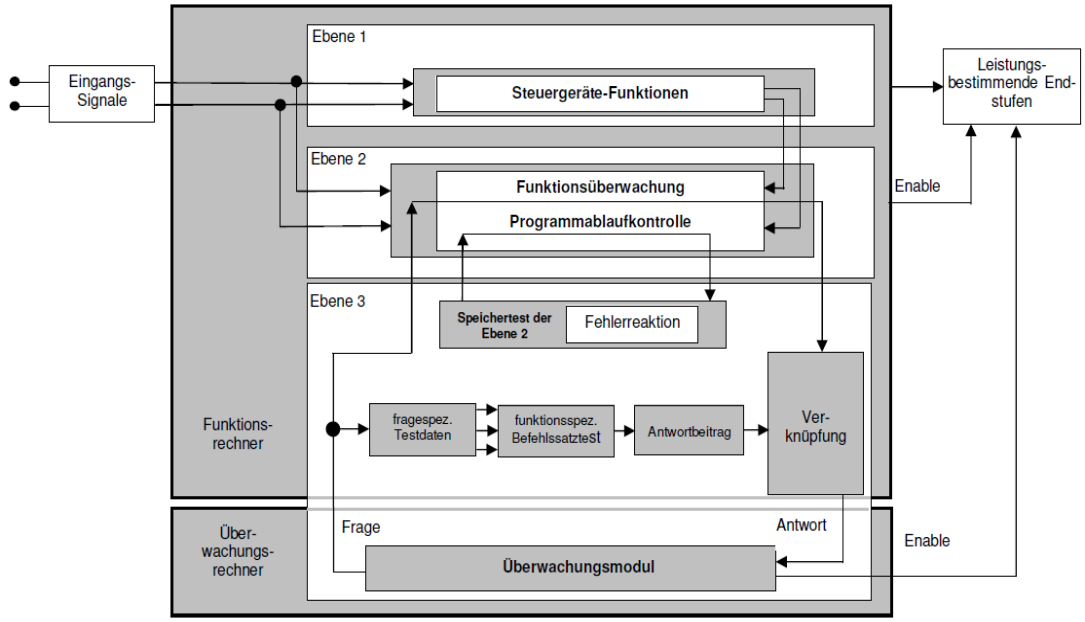



Abbildung 4.2: EGAS Basiskonzept der Robert Bosch GmbH, Quelle: [58]

Die Überwachung bei EGAS erfolgt stets in drei Ebenen:

**Ebene 1** wird als Funktionsebene bezeichnet. Sie beinhaltet die eigentlichen Funktionen, bei einer Motorsteuerung z.B. zur Umsetzung der angeforderten Motormomente, Kompo-

[50] Selbst elektrische Lenksysteme wurden über von EGAS abgeleitetete Sicherheitskonzepte abgesichert, wobei gesagt werden muss, dass mit EGAS heute schwerlich ASIL D erreicht werden kann. Die Zeitanforderungen für Überwachungen und FTTI liegen um etwa eine Zehnerpotenz voneinander entfernt (Lenkung 10ms).

nentenüberwachungen, die Diagnose der Ein- und Ausgangsgrößen, sowie die Steuerung der Systemreaktionen im erkannten Fehlerfall.

**Ebene 2** wird als Funktions-Überwachungsebene bezeichnet. Sie erkennt den fehlerhaften Ablauf überwachungsrelevanter Umfänge der Funktionssoftware in Ebene 1, unter anderem durch die Überwachung der berechneten Sollwerte. Im Fehlerfall erfolgt die Auslösung von Systemreaktionen.

**Ebene 3** wird als Rechner-Überwachungsebene bezeichnet. Hauptbestandteil ist eine vom Funktionsrechner unabhängige Hardware zur Überwachung, welche durch ein Frage-Antwort-Verfahren die ordnungsgemäße Abarbeitung der Programmbefehle im Funktionsrechner überprüft. Im Fehlerfall erfolgt die Auslösung von Systemreaktionen zur Deaktivierung der Aktorik unabhängig vom Funktionsrechner.

Ebene 3 besteht aus 2 verschiedenen Elementen, die über eine Schnittstelle kommunizieren:

- einem physikalisch unabhängigen Überwachungsmodul (E3_ÜM) und
- einer Überwachungssoftware (E3_SW) im Funktionsrechner (FR).

Das Modul E3_ÜM stellt der Software E3_SW im FR zyklisch eine Frage aus einer Menge von mindestens 10 verschiedenen Fragen, überwacht den Empfang eines zyklischen Prüfergebnisses, bewertet dieses und leitet im Fehlerfalle eine Fehlerreaktion ein. Das Überwachungsmodul kann dabei als *Application Specific Integrated Circuit* (ASIC) oder als *System Basis Chip* (SBC) realisiert sein. Bei Verwendung von RAM/ROM-Bausteinen in E3_ÜM sind diese durch E3_ÜM mindestens einmal je Fahrzyklus zu testen.

Die Interaktion zwischen E3_ÜM und E3_SW im FR wird auch als Frage-Antwort-Kommunikation bezeichnet. Dabei werden mehrere Testpfade im Funktionsrechner abgearbeitet. Jeder Testpfad liefert ein exakt definiertes, frageabhängiges numerisches Teilergebnis. Die Verknüpfung der Teilergebnisse führt zu einem numerischen Gesamtergebnis (Prüfergebnis), welches per Kommunikationsschnittstelle an E3_ÜM übertragen wird. E3_SW im FR signalisiert dem Modul E3_ÜM durch richtige Antworten den fehlerfreien Betrieb. Auf diese Weise stellt E3_ÜM eine Art intelligenten Watchdog mit eigener HW zur Funktionsabschaltung (In Aktornähe UND-verknüpfte Enable-Leitungen, die im Fehlerfall deaktiviert werden) dar.

Zur Ebene 3 gehören z.B. folgende Überwachungen und Tests als SMs:

- Überwachung der Frage-/Antwort-Kommunikation mit Wiederholrate unter 80ms
- Testpfade der Software E3_SW im Funktionsrechner (Programmablaufkontrolle; funktionsspezifischer Befehlssatztest)

- Randomisierte Fragegenerierung in E3_ÜM
- Überwachung des Echtzeitsystems (en: Timing Processing Unit[51], TPU) mit seinem Zeitparameterspeicher und seinem Arbeitsspeicher (RAM, zyklisch überwacht) und Festwertspeicher (ROM, einmal pro Fahrzyklus überwacht)
- Prüfung der Abschaltpfade mindestens einmal im Fahrzyklus
- A/D-Wandlertest gegen Steigungsfehler, Offsetfehler und Stuck-At-Fehler[52]

Sichere (Zwischen-)Zustände werden durch das Zurücksetzen (Reset) von Überwachungsmodul (E3_ÜM) und Funktionsrechner (FR) und durch das Abschalten der leistungsbestimmenden Endstufen definiert. Die Dauer des Reset-Status muss projekt- bzw. produktspezifisch festgelegt werden.

## 4.7 Ende zu Ende-Absicherung und das Gray-Channel Prinzip

Zur Absicherung von Signalübertragungen und der Kommunikation von Daten gibt es verschiedene Mechanismen (SMs) und Prinzipien. Viele davon wurden in Abschnitt 2.4 in Zusammenhang mit anderen elektronischen Baugruppen bereits genannt. Das Spektrum reicht von Ein- oder Mehr-Bit-Redundanz mit z.B. beigefügten Parity-Bits über komplette Datenredundanz oder später inspizierte Testmuster und Codesicherungen bis hin zu mehrkanaliger, paralleler, zyklischer oder wiederholter Übertragung und/oder Übertragungsredundanz, möglicherweise mit antivalenten oder invers übertragenen Daten. Ausbleibende Daten, sofern das bezüglich sicheren Zustands nicht passieren darf, müssen hinsichtlich ihres Empfangs zeitlich überwacht werden (Timeout). Zur Aufdeckung von irrtümlich wiederholten bzw. falsch zugestellten Botschaften werden der Übertragung Botschaftszähler und Identifikationsnummern beigefügt. Zur Diagnosedeckung der verschiedenen Fehlerarten und –möglichkeiten muss eine Kombination der genannten SMs angewandt werden.
Folgende Aspekte und Fehlerquellen beim Austausch von Information, beispielsweise bei der Übertragung von Lenkwinkelsensordaten über ein Bussystem an ein EPS-Steuergerät, müssen betrachtet und entsprechende Fehler zur Laufzeit beherrscht werden.

- Wiederholung derselben, „hängengebliebenen“ Informationen (en: repetition)
- Verlust von Informationen (en: loss)
- Verzögerung der Information (en: delay)

[51] Manchmal wird dies z.B. durch separierte Hardware, einen Co- oder Subprozessor realisiert.
[52] Diese entstehen z.B. durch das „Einfrieren“ von Registern oder des Kanalmultiplexers (MUX).

- Einfügung unerwünschter Informationen (en: insertion)
- Falsch adressierte oder irrtümliche Zustellung (en: masquerade)
- Falsche Reihenfolge der Informationen (en: incorrect sequence)
- Korrupte, zerstörte oder verstümmelte Informationen (en: corruption)
- Falsch verteilte Informationen
- Versperrter Zugriff auf Übertragungskanäle und -medien (en: blocking access)

Zur Absicherung gegen alle diese Fehlermöglichkeiten müssen entsprechende SMs auf Senderseite provisioniert werden, d.h. ohne den Gesamtentwurf für Sender und Empfänger kann auf Empfängerseite nichts überwacht und beherrscht werden.
Bei der Übertragung von Lenkwinkelsensordaten über ein im Automobilbereich übliches Bussystem wie CAN oder Flexray werden die hierfür kritischen Fehlerquellen in der Regel durch einen mehr oder minder streng in seiner Reihenfolge überwachten Botschaftszähler, eine eindeutige Botschaftsidentität (ID) und einen ausreichend starken[53], über die gesamten Botschaftsinhalte verlaufenden CRC kontrollierbar gemacht.

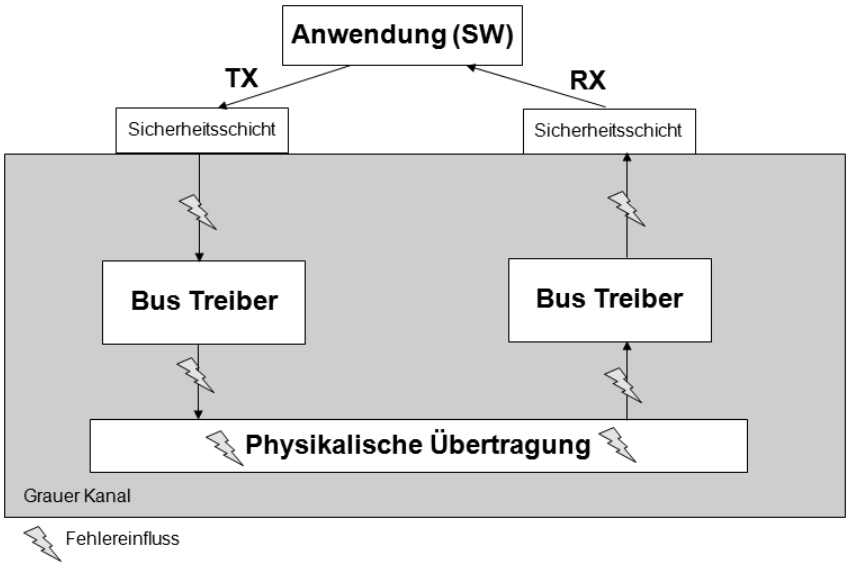



Abbildung 4.3: Datenübertragungsweg als grauer Kanal mit umgebender Sicherheitsschicht

Grundsätzliches Prinzip bei jeder gesicherten Datenübertragung ist es, einen möglichst langen, über möglichst weite Teile laufenden Übertragungsweg von einem Ende zum anderen Ende zu entwerfen, weil so alle Fehler, die zwischen Einbringung der Mechanismen auf Senderseite und ihrer Auswertung auf Empfängerseite eingestreut werden oder passie-

[53] Entscheidend ist eine möglichst hohe Hamming-Distanz.

ren, aufgedeckt und weitere Aufwände für den abgedeckten Weg vermieden werden können. Die genannten Mechanismen werden daher gern schon auf Anwendungsebene in der SW provisioniert und auch erst wieder auf Anwendungsebene in der SW des Empfängers ausgewertet. Man spricht bei den den gesamten Übertragungsweg abdeckenden SMs von einer Ende-zu-Ende-Absicherung (en: end-to-end protection, E2E) oder auch von einer den Übertragungsweg umgebenden Sicherheitsschicht (en: safety shell), wie Abbildung 4.3 verdeutlicht. Der durch die vorgesehenen SMs (E2E) eingeschlossene Übertragungsweg wird manchmal „grauer Kanal“ (en: grey-channel) genannt [59], weil er einen extern ausreichend abgesicherten Bereich darstellt, innerhalb dessen man keine weiteren SMs vorsehen muss. Abbildung 4.4 nach [60] macht deutlich, wie im Übertragungsweg auch die Fehler in Softwareteilen und -schichten, in Treiberschichten, in der Transceiver-HW und dem physikalischen Bussystemen aufgedeckt und beherrscht werden können, wenn die SMs bereits auf Anwendungsebene provisioniert und am anderen Ende erst wieder auf Anwendungsebene ausgewertet werden.

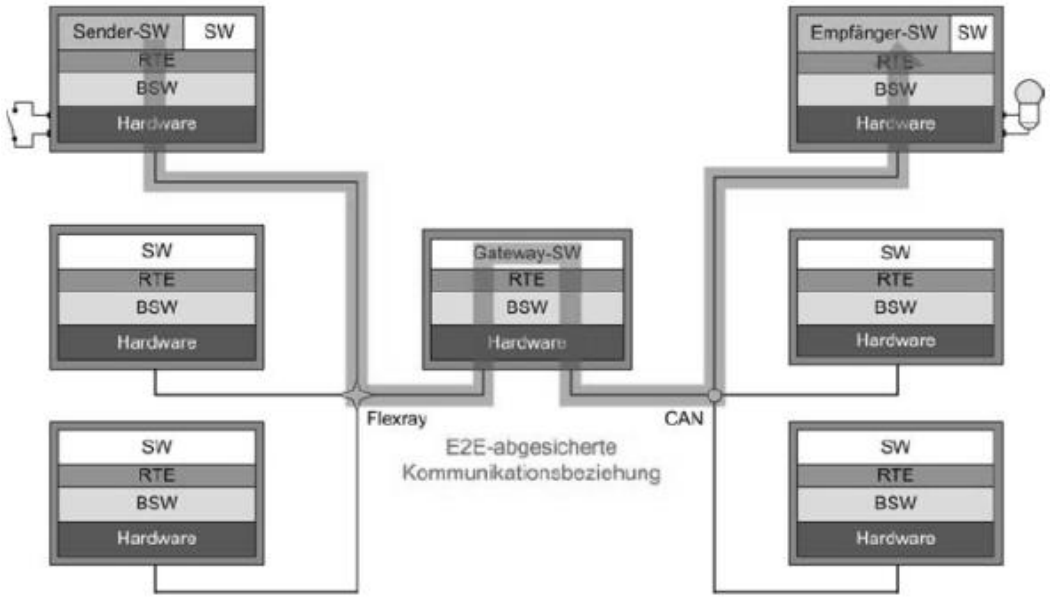



Abbildung 4.4: E2E Absicherung über verschiedene Bussysteme hinweg, nach [60]

Die Enden des Kommunikationsweges mit ihren Absicherungsmechanismen sind die Softwareanwendungen auf oberster, funktionaler Ebene. Die Abkürzungen BSW und RTE

in der Abbildung stehen für die Basissoftware[54] bzw. für die Laufzeitumgebung (en: runtime environment) wie sie z.B. durch ein Echtzeitbetriebsystem (RTOS) gegeben ist.

## 4.8 DEGRADATIONSKONZEPTE UND NOTLAUF

Nach der Aufdeckung eines Ausfalls von HW zur Betriebszeit gibt es Situationen, in denen die Gesamtfunktionalität des Items oder gar das Fahrzeug nicht augenblicklich ab- bzw. energielos geschaltet werden darf. Stattdessen muss die Funktionalität schrittweise eingeschränkt und degradiert werden (en: graceful degradation), sodass das Fahrzeug für die Fahrzeugführenden gerade sicher beherrschbar bleibt, bis die Werkstatt oder wenigstens der Stillstand des Fahrzeugs am Straßenrand erreicht wurde. Man spricht in diesen Fällen auch von selektiver Abschaltung (en: selective shut off) und bei eingeschränkter Fahrt von einem Betrieb unter Notlaufeigenschaften oder kurz von Notlauf (en: limp home).

Ein Notlauf mit sicherheits- und vielleicht auch funktionsbezogener Einschränkung muss den Fahrzeugführenden vermittelt werden, um ihnen (wieder) einen größeren Teil der Sicherheitsverantwortung für die Weiterfahrt zu übertragen und erhöhte Vorsicht zu gebieten. Die Warnung ist meist ein kurzes oder wiederkehrendes, akustisches oder taktiles[55] Signal, ergänzt durch eine Signalanzeige.

Degradation in Zusammenhang mit einem Lenkwinkelsensor kann darin bestehen, dass bestimmte, vom Lenkwinkelsensor abhängige Funktionalitäten oder Teilfunktionen abgeschaltet werden. Sendet der Lenkwinkelsensor überhaupt keine Messdaten mehr aus oder ist die Kommunikation gänzlich unterbrochen, müssen abhängige Funktionalitäten (von Safety Items) komplett abgeschaltet werden. Eine (eingeschränkte) Weiterfahrt ist nur dann denkbar, wenn es sich um eine zusätzliche, elektronische Assistenzfunktionalität handelte und eine beispielsweise mechanisch wirkende Rückfallebene existiert, auf die dann zurückgegriffen werden kann. Eine geschwindigkeitsabhängige Lenkübersetzung oder ein ESP mit Lenkeingriffen wären Beispiele hierfür. Der plötzliche Wegfall der Assistenz bzw. Zusatzfunktionalität sollte in jedem Fall angezeigt werden.

Für ein differenzierteres Degradations- oder Notlaufkonzept werden nur einzelne Teilfunktionen oder Effekte zurückgenommen. Um dies zu ermöglichen, muss den Steuergeräten, die den Lenkwinkel empfangen, die Möglichkeit zur differenzierten Entscheidung gegeben werden. Wird der Lenkwinkel für das betroffene Item unbedingt benötigt? Oder

[54] Die BSW besteht meist aus im Rahmen von Autosar (AUTomotive Open System ARchitecture) standardisierten Software- und Treiber-Bibliotheken zum Betrieb einer ECU als Netzknoten an einem der üblichen Bussysteme CAN oder Flexray.
[55] Z.B. durch Lenkradvibration

wird der Lenkwinkel zwar benötigt, aber vielleicht zur Not nur mit geringerer Sicherheitsintegrität oder nur mit geringerer Genauigkeit? Für diese Zwecke muss das LWS-Modul bei interner Fehlererkennung in der Lage sein, neben den Messwerten zu kommunizieren, welche Art Fehler genau aufgetreten sind oder ob und wie sich Messwerttoleranzen erhöht oder –genauigkeiten verringert haben.

Wenn im LWS bestimmte SMs ausfallen, könnte zwar die Messgenauigkeit unverändert geblieben sein. Trotzdem muss es mindestens zur Degradation der abhängigen Funktionalität kommen, denn die volle Sicherheitsintegrität ist nicht mehr gegeben. Zu diesem Zweck muss der erkannte Fehler derart an das angeschlossene Steuergerät kommuniziert werden, dass dieses entweder den Grad des Verlusts der Sicherheitsintegrität einordnen kann oder dass ihm die verminderte Qualität oder Sicherheitsintegrität der Messdaten direkt mitgeteilt wird. Bekannt ist dieses Verfahren mit der Übertragung eines entsprechenden „Qualifiers“. Das Patent DE 10 2009 019792 [61] beschreibt zu diesem Thema einen mit den Funktionsdaten zusammen übertragenen Wert, der den angeschlossenen Steuergeräten direkt den jeweils erreichten ASIL für die übertragenen Signale oder Daten zur weiteren Entscheidung über Abschaltung oder Degradation angibt.

Beispiel für eine solche Degradation könnte ein ESP sein, das bei Einschränkung der Sicherheitsintegrität des Lenkwinkels im Fall der Fahrzeuginstabilität nur noch Bremseingriffe, aber keine korrigierenden Lenkeingriffe mehr vornimmt. Sehr kritische Funktionalitäten bzw. Items mit ASIL C und D behafteten SZs müssen unter Umständen komplett still geschaltet werden, während z.B. das kurvenadaptive Abblendlicht bei ASIL B oder die Müdigkeitserkennung bei weiterer Reduzierung der Integrität des Lenkwinkelsignals auf ASIL A weiter arbeiten könnten. Eine verminderte Genauigkeit des gemessenen Lenkwinkels würde vielleicht die SZs einer elektronischen Blinkerrückstellung nicht verletzen, sodass diese gegebenenfalls unverändert aktiv bleiben darf.

# 5 LENKWINKELSENSOREN

Lenkwinkelsensoren (LWS) werden zur Realisierung verschiedenster Funktionalitäten im Automobil eingesetzt. Unmittelbar hinter dem Lenkrad positioniert nehmen sie den Fahrtrichtungswunsch des Fahrers auf. Andere Varianten, unten hinter dem Lenkgetriebe oder auch am Motor der EPS erfassen den tatsächlichen Lenkeinschlag. Als Komponente, die im Bereich der Sensorik wie keine andere Einfluss auf die Querdynamik des Fahrzeugs hat, werden LWS in der Regel in irgendeiner Form sicherheitsbezogen verwendet, sobald es um Funktionalitäten geht, die Fahraktorik und Fahrzeugdynamik beeinflussen. Unter den zahlreichen, modernen und elektronisch unterstützten Funktionalitäten mit Lenkwinkeldaten befinden sich zum Beispiel das der Fahrtrichtung elektronisch angepasste Scheinwerferlicht, Einparkhilfen, verschiedene Stabilitätsprogramme mit Brems- und Lenkeingriffen, der Fahrzeuggeschwindigkeit angepasste Lenkkraftverstärkungen oder Lenkgetriebeuntersetzungen[56] und Hinterachslenkungen bis hin zum vollelektronisch angesteuertem Lenken (Steer-by-wire). Aber auch unter Umständen unkritische Funktionalitäten wie Navigationsaufgaben, die automatische Blinkerrückstellung, Müdigkeitserkennungen und viele andere Assistenzfunktionen sind auf die vom LWS ausgegebenen Daten angewiesen.

## 5.1 ANFORDERUNGEN AN SICHERHEITSGERICHTETE LENKWINKELSENSOREN

Die Anforderungen an den LWS zum Einsatz im Kraftfahrzeug sind vielfältig. Neben den schon erläuterten Anforderungen an die Funktionssicherheit stehen natürlich grundsätzlich die eigentlichen Funktionsanforderungen der ausreichend genauen Erfassung der Lenkposition oder -änderung und die der beabsichtigten Qualität und Zuverlässigkeit [62].
Ein LWS am Lenkrad muss die Position des Lenkrades in der Regel über mehrere (4 bis 5) Lenkradrunden hinweg mechanisch derart abbilden, dass sie absolut, d.h. über die Runden eindeutig gemessen und ausgegeben werden kann. So entsteht ein Messbereich von z.B. 0 bis 4 mal 360°, also je nach Winkelausgabenormierung von -720° für den Vollausschlag nach links, 0° für beabsichtigte Geradeausfahrt und +720° für einen Vollausschlag Rechts. So manche Funktionalität benötigt von einem LWS nur die Winkeländerungsdynamik oder auch bloß die Winkeländerungen, d.h. relative Winkelangaben.
Auf Genauigkeit und die Art möglicher Messfehler haben Hysterese durch mechanisches Spiel und Elastizität, integrale und differenzielle Nichtlinearität, Offset und externe Einflüsse wie Temperaturwechsel großen Einfluss [62].

[56] Auch Aktivlenkung, Dynamiklenkung oder Überlagerungslenkung genannt.

Allgemein spielt bei einer Komponente, einem mechatronischen Modul im Seriengeschäft der Automobil- und Automobilzulieferindustrie, der Kostenaspekt gleich nach der funktionalen Sicherheit eine herausragende Rolle. Bei hohen Stückzahlen müssen insbesondere Material und Herstellung kostengünstig ausgelegt sein [62].
Bezüglich Materials kommt es besonders auf Zahl und Größe der mikroelektronischen Einzelkomponenten an, weil diese Bauteile meist hochkomplex und teuer im Einkauf sind. Ein einfacher, wenig komplexer Entwurf mit möglichst wenigen, mikroelektronischen Komponenten ist aber auch der Weg zu besonders hoher Sicherheitsintegrität.
Bezüglich kostengünstiger Herstellung gilt das Gebot einfacher und möglichst schneller Fertigungsprozesse. Vor allem Zwischen- und Bandendeprüfungen, wie auch in der Regel notwendige Kalibrierungen, werden zeitoptimiert ausgelegt.
Weitere Anforderungen betreffen den Bauraum der Messvorrichtung, der nicht immer nur generell klein gehalten, sondern manchmal auch spezifische Formen im Bereich des Einbauorts einhalten soll oder eine bestimmte Geometrie nicht überschreiten darf.
Allgemeine Anforderung, z.B. an einen geringen elektrischen Leistungsbedarf im Betrieb und im Ruhezustand, an eine maximale Geräuschentwicklung oder hinsichtlich weitgehender Wartungsfreiheit kommen stets hinzu und runden das Bild für ein brauchbares Sensormodul für Lenkradpositionen ab.

## 5.2 Mechanische und elektrotechnische Grundlagen der magnetischen Lenkwinkelmessung

### 5.2.1 Exzentrische Erfassung mehrperiodischer Lenkbewegungen

Für viele Funktionalitäten im Fahrzeug ist es notwendig, den Fahrtrichtungswunsch der Fahrzeugführenden möglichst unmittelbar zu ermitteln, also ohne mechanikbedingtes Spiel direkt am Lenkrad. Mechanische Spiele in der Lenksäule und im Lenkgetriebe würden die Lenkwinkelinformation ungenauer machen oder verfälschen.
Wegen der Lenksäule, um die das Sensormodul (en: Steering Angle Sensor, SAS) montiert wird, muss in der Regel zudem exzentrisch gemessen werden, d.h. es wird eine Mechanik benötigt, die das Rotorsignal des Lenkrades über die Lenkspindel an den außenliegenden Stator Lenksäule mit der Messeinrichtung überträgt. Als Lenkradwinkel erfasst wird dann der Winkel zwischen der Lenkspindel als Rotor, mit dem das Lenkrad fest verbunden ist, und dem außen liegenden Vorrichtungsgehäuse an der Lenksäule als Stator und Bezugspunkt [62].
Außerdem geht es darum, nicht nur relative 360° einer einzelnen Lenkradrunde, sondern die vier bis fünf üblichen Runden eines Lenkrades in einem absoluten Winkel zu erfassen.

Die ermittelten Absolutwinkelwerte werden anschließend in aller Regel über ein digitales Bussystem und den im Fahrzeugsystem höchsten Sicherheitsansprüchen entsprechend Ende-zu-Ende abgesichert zur Weiterverarbeitung versendet. Als Bussystem im Kraftfahrzeug sind Local Interconnect Network (LIN), Controller Area Network (CAN) oder Flexray üblich. Ein Betrieb bei Ausfall des Bussystems, der entsprechenden Botschaften oder bei inkonsistenten Botschaften (fail operational) der einen Komponente ist bislang unüblich. Ein Notlauf für zeitlich begrenzten Betrieb mit eingeschränkter Sicherheitsintegrität wird – wenn überhaupt - durch autarke Botschaften von Komponenten mit gleichen Daten an anderen Verbauorten ermöglicht.

### 5.2.2 Kleiner Bauraum und mikroelektronische Unterstützung

Beim Einsatz einer mechanisch-magnetisch-elektronischen Signalumsetzung kommen als Sensorchip Hall-Sensoren zum Einsatz, die den Winkel eines Magnetfeldes im zwei- oder sogar dreidimensionalen Raum erfassen können. Der gesamte Bauraum einer Messvorrichtung wird einerseits durch die mechanische Anpassung und durch die für die Messtechnologie notwendige Umsetzung bestimmt. Eine Messung per Induktionsprinzip beispielsweise benötigt entsprechende Spulensysteme. Ein magnetisches Prinzip benötigt ein in die Drehmechanik eingebrachtes Magnetsystem. Andererseits liegt zur Minimierung des Bauraums einiges an den Abmaßen der am Markt verfügbaren Mikrosensorik und Mikroelektronik, die zur Anwendung im Automobil geeignet und einsetzbar ist.

Für den Einbauort eines LWS-Moduls direkt unterhalb des Lenkrades an der Lenksäule, also innerhalb der Fahrgastzelle im Automobil, wird zur Qualifizierung üblicherweise ein Temperaturprofil mit Temperaturen zwischen -40 Grad Celsius und +85 Grad Celsius spezifiziert. Im Gegensatz dazu liegen Temperaturbereich und damit zusammenhängend auch die Kosten eines Sensormoduls für Einbauorte im Motorraum deutlich höher [62].

Die mikroelektronische Unterstützung für ein Lenkradwinkelsensormodul besteht aus der möglichst rückwirkungsfreien, also berührungslosen Erfassung der Winkelposition des Lenkrades durch einen Analogteil und aus einem „intelligenten“ Digitalteil. Der digitale Bereich einer solchen Schaltung ist einerseits für die Messalgorithmik und die Ausgabe der Messergebnisse über eine digitale Schnittstelle zuständig und muss andererseits Eigendiagnostik und Fehlerbeherrschungsmaßnahmen leisten können, um die gewünschte Sicherheitsintegrität aufzubringen. Infrage kommt hier z.B. der im dreidimensionalen Raum messende, integrierte Schaltkreises (en: integrated circuit, IC) *MLX90363* der Firma Melexis N.V., der in Zusammenarbeit mit dem Verfasser für die Firma KOSTAL GmbH & Co KG zum Zwecke ähnlicher Aufgaben in zweidimensionaler Anwendung entwickelt und bereits mit etlichen, notwendigen Sicherheitsmerkmalen versehen wurde.

Der nächste Abschnitt soll an dieser Stelle einen Überblick über die Ausführung und die Möglichkeiten eines solchen Chips geben.

### 5.2.3 MIKROELEKTRONISCHE HALL-SENSORIK

Für einen auf Magnettechnologie basierenden LWS wird ein moderner Hall-Sensorschaltkreis wie der im vorigen Abschnitt bereits erwähnte MLX90363 benötigt. Um die Anforderungen und Möglichkeiten eines solchen mikroelektronischen Bausteins besser zu verstehen, soll im Folgenden speziell auf dieses IC eingegangen werden.
Der MLX90363 ist ein IC mit sogenanntem *Rotary Position Sensor*, der eine serielle Schnittstelle (Serial Peripheral Interface, SPI) für hohe Datenraten integriert. Abbildung 5.1 zeigt das entsprechende Blockschaltbild dieses ICs mit integrierter Spannungsversorgung, Hall-Sensorik, differenziell arbeitendem Analogverstärker, einem Analog-Digital Wandler (ADC) und dem digitalen Signalprozessor (DSP) im Digitalteil auf der rechten Seite.

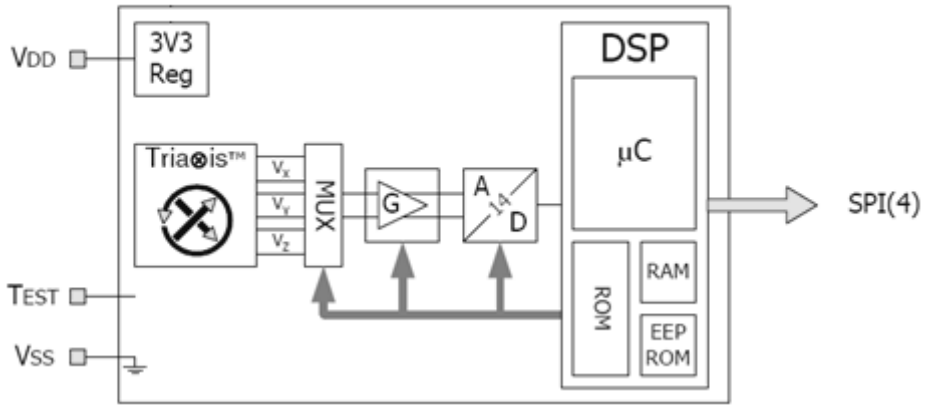



Abbildung 5.1: Blockschaltbild MLX90363, [63], Seite 1

Der Baustein integriert laut Datenblatt [63] folgende Eigenschaften und Vorteile.

- Einfache und robuste magnetische Ausführung
- Dreidimensional im Raum erfassende Hall-Technologie (Tria⊗is™)
- Vollständiger Winkelbereich bis 360 Grad
- Bis 2 MHz taktbare und voll duplex betreibbare serielle Schnittstelle (SPI)
- 14 Bit Winkelauflösung - 10 Bit Winkelgenauigkeit im Temperaturbereich
- 48 Bit Identifizierungnummer
- Eine einzige Siliziumhalbleiterfläche (Die) im SO8 Gehäuse mit 8 Anschlüssen

- Erweiterte Eigenschaften für Selbstdiagnose
- 5V und 3,3V Anwendung möglich, spannungsfest bis zu 18 Volt

Das Layout des räumlich messenden Hall-Sensorschaltkreises zeigt neben der Hall-Sensorik und den Analogteilen vor allem die Baugruppen eines typischen Computers in Von-Neumann-Architektur. Beim MLX90363 ist ein vollständiger Mikrocontroller mit 16 Bit Datenverarbeitungsbreite als IP-Block (en: intellectual property) integriert.
Da Hall-Sensorik und ihre Genauigkeit sehr temperaturabhängig ist, wird die Temperatur auf dem Chip redundant erfasst und zur Winkelmessung kompensierend einbezogen.
Die eigentliche Hall-Sensorik in dem IC besteht aus einer ferromagnetischen Scheibe, dem sogenannten Integrierten Magnetfeld-Konzentrator (IMC) und mindestens vier darum liegend angeordneten Hall-Effekt-Platten.
Der gesamte Sensorchip benötigt eine Silizium-Die-Fläche von lediglich etwa 1,8 x 1,8 $mm^2$. Größe und Leistungsumfang machen den bereits hohen Integrationsgrad dieses ICs deutlich. Schaltungsstrukturen in Nanometerbereichen und mit neuen Fertigungstechnologien können sich wegen erhöhter Ausfallempfindlichkeit und naheliegend höherer Basisfehlerraten wieder nachteilig für die Sicherheit auswirken.

### 5.2.4 SIGNALVERARBEITUNG

Ein Hall-Sensorschaltkreis wie der MLX90363 ist empfindlich in mindestens zwei Dimensionen der magnetischen Flussdichte, der der Baustein durch ein sich drehendes Magnetsystem ausgesetzt ist, d.h. mindestens in einer Ebene mit $B_X$ und $B_Y$. Diese Eigenschaft ermöglicht es ihm die Winkelposition eines Magnetfeldes zu den Ebenen im Raum von 0 bis 360 Grad zu dekodieren oder allgemeiner ausgedrückt, jede Drehbewegung eines Magneten in seiner Umgebung genau zu bestimmen, ohne in direktem Kontakt mit dem aufzunehmenden Signal zu stehen.
In Kombination mit einer integrierten Signalverarbeitung kann die magnetische Flussdichte eines um das IC herum bewegten Messrades mit darin enthaltenem Magnetsystem berührungslos gemessen werden. Prinzipiell werden dabei analoge Hall-Spannungen nach der Digitalwandlung dem integrierten Signalprozessor zur weiteren Verarbeitung zugeführt. Hauptaufgabe dieses RISC-basierten Mikrocontrollers ist die Ermittlung und serielle Ausgabe von Winkelinformationen im Bereich 0° bis 360°. Für Details wird an dieser Stelle auf die entsprechenden Datenblätter und die Ausführungen in [62] verwiesen.
Die Funktionalität des Signalprozessors wird über einen Mikrocode (Firmware – FW) gesteuert, welcher in einem internen Festspeicher (en: Read Only Memory, ROM) fest

einprogrammiert ist. Neben der Aufgabe der Berechnungen der konfigurierbar gewünschten Winkelwerte über trigonometrische Funktionen steuert die Firmware die komplette Analogverarbeitungskette, die Kalibrierung und Programmierung der Parameter, die Kommunikation über die digitale SPI-Schnittstelle und auch die verschiedenen, eingebauten Fehleraufdeckungsmechanismen[57].

Die Programmierung aller notwendigen Parameter kann über einzelne Befehle des umfangreichen Protokolls via SPI erledigt werden. Eine SPI-Schnittstelle beruht auf einer Master-Slave Konstellation, was bedeutet, dass die an einen als Master fungierenden Mikrocontroller angeschlossenen Peripheriebausteine stets auf Anforderungen warten und niemals von sich aus die Initiative für den Datenaustausch ergreifen (Slave).

Der Baustein MLX90363 unterstützt ein serielles Protokoll mit 64 Bits pro Telegramm in beiden Richtungen. Dieses Protokoll ermöglicht eine gesicherte Übertragung der ermittelten Winkelwerte nach außen zur weiteren Verarbeitung im Gesamtsystem. So sieht das Übertragungsprotokoll z.B. als Maßnahme gegen Maskerade einen sogenannten Operationscode als Telegramm-Identifikation, eine 8 Bit breite CRC-Prüfsumme[58] mit C2 Polynom zur Aufdeckung korrupter Daten und einen bis zu 6 Bit breiten Botschaftszähler zur Überprüfung aktueller und zeitgerechter Daten beim Empfänger vor. Hier bietet nach dem Stand der Technik der Sensorbaustein bereits intrinsisch alle Möglichkeiten zu einer sicheren Übertragung der Messdaten, selbst wenn diese für bestimmte SZs mit Integrität der Stufe ASIL D erforderlich wären.

## 5.3 Moderne magnetische Lenkwinkelsensoren

In Kraftfahrzeugen müssen zur Messung der absoluten Position des Lenkrades über mehrere Runden hinweg Sensormodule eingesetzt werden, die einerseits kostengünstig sind und andererseits ausreichend genau, zuverlässig und funktional sicher arbeiten. In einem solchen LWS wird die jeweils absolute Position des Lenkrades durch eine mehrperiodische Kreiswinkelmessung bestimmt. Da sich das Lenkrad in aller Regel mit seiner Achse, der Lenkspindel, kugelgelagert innerhalb der Lenksäule dreht und nicht um die Lenksäule herum, kann die Lenkbewegung nicht zentrisch gemessen werden und muss über eine geeignete Umsetzung zum außen liegenden Stator als Bezugspunkt überführt werden.

Magnetisch arbeitende LWS sind heute international, z.B. in Fahrzeugen von GM, Ford, Volkswagen, Audi, BMW oder Toyota weit verbreitet.

[57] Diese ergeben sich direkt oder indirekt aus den jeweiligen Datenblättern.

[58] C2 (0x97= $(x+1)(x^7+x^6+x^5+x^2+1)$) nach Baicheva [82] bis 119 Bit Datenlänge mit einer Hemmingdistanz von 4 [81]

### 5.3.1 STAND DER TECHNIK UND DAS NONIUSPRINZIP

Lenkwinkelsensormodule für Automobile beruhen heute auf verschiedenen Prinzipien (vgl. [64]). Hier sind zum einen auf Potenziometer basierte Systeme und auch optisch, induktiv oder magnetisch arbeitende Systeme zu nennen. Die Mehrperiodizität des Lenkrades (in Runden) wird oft über eine separierte mechanische Einrichtung, z.B. mit Schneckentrieb erfasst oder auch über eine Kombination aus optischer, induktiver und magnetischer Sensorik. Manchmal wird nur der relative Lenkwinkel innerhalb einer Drehung um 360° erfasst und die jeweilige Runde des Lenkrades ergibt sich durch eine Auswertung der in Kurven unterschiedlichen Raddrehzahlen an der gelenkten Fahrzeugachse.
Mit einer Patentschrift [65] von 2008 ist eine absolut messende Drehwinkelmessvorrichtung bekannt, die den absoluten Drehwinkel mit mindestens zwei Magnetsensoren über mehrere Runden erfassen kann. Abbildung 5.2 zeigt das geöffnete Gehäuse eines solchen, heute üblichen Lenkwinkelsensormoduls mit Magnettechnologie.

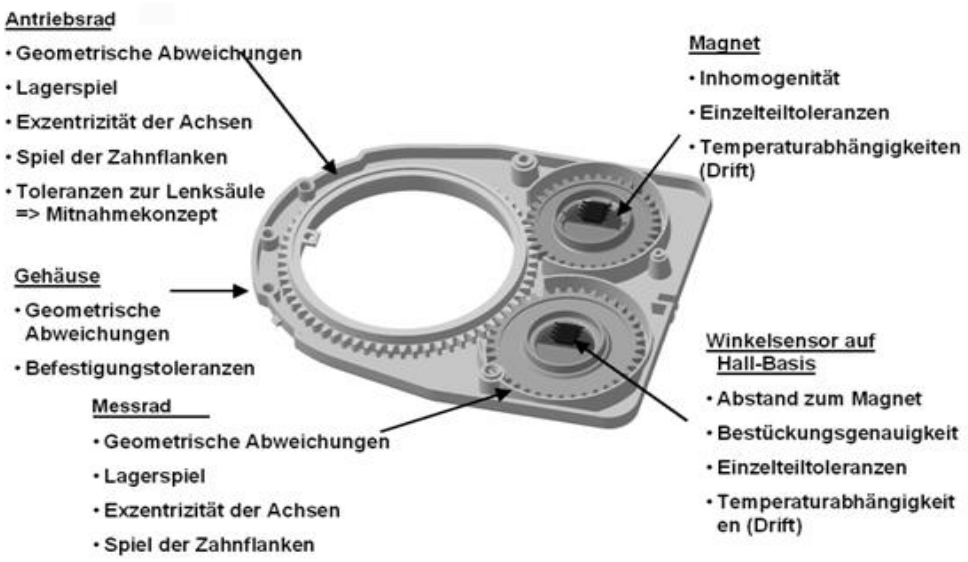



Abbildung 5.2: Üblicher Lenkwinkelsensor, exzentrisch messend. Dieser erfasst Absolutwinkel über mindestens 5 Runden in der Lenksäulenachse nach dem Noniusprinzip und mittels zweier Hall-Sensor-ICs.

Durch Abbildung 5.2 werden die in Abschnitt 5.1 genannten Abhängigkeiten für die Genauigkeit und mögliche Fehlerursachen bei einem LWS-Modul verdeutlicht.
Zur Anwendung hierbei kommt das sogenannte Noniusprinzip[59], das auch unter dem Namen des französischen Mathematikers und Erfinders Vernier[60] bekannt ist und vor allem –

[59] Die in deutschsprachigen und anderen Ländern übliche Bezeichnung Nonius geht auf den portugiesischen Astronomen, Mathematiker und Geografen Pedro Nunes (latinisiert: Petrus Nonius; 1502–1578) zurück, der den Nonius jedoch nicht erfunden hat [66].

und das war das ursprüngliche Ziel bei der Entdeckung des Prinzips im Mittelalter – genutzt wird, um die Genauigkeit der Messungen zu erhöhen [66].
Aus der Schwebung zwischen zwei unterschiedlich frequenten Einzeldrehungen lassen sich absolute Winkel bestimmen, die über die jeweils 360° einer Einzeldrehung hinausgehen. Dabei werden unter zwei verschieden großen Messrädern mit elektronischen Hall-Sensoren zwei Winkel bestimmt, die zur Erfassung eines absoluten Winkels am gemeinsamen Antriebsrad um die zu messende Drehachse kombiniert werden können [62].
Abbildung 5.3 zeigt die schematische Darstellung eines solchen Lenkwinkelsensormoduls.

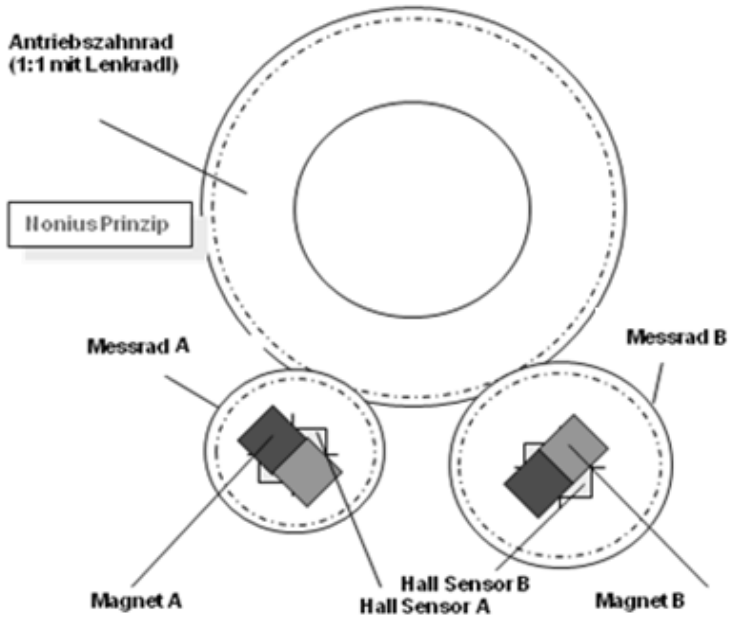



Abbildung 5.3: Schematische Darstellung eines magnetischen Lenkwinkelsensormoduls

Die beiden separat und in derselben Ebene gelagerten Messräder werden beispielsweise über die Verzahnung eines Zahnradgetriebes oder die Haftreibung einer Gummibeschichtung angetrieben und stehen so zueinander in einem festen Übersetzungsverhältnis.
Das Noniusprinzip wird im Bereich der Automobiltechnik zur Messung sicherheitskritischer Größen zunehmend verbreitet eingesetzt, nicht nur zur Lenkwinkelerfassung. Bei der berührungslosen Erfassung von Lenkwinkeln mit Magnettechnologie ist das Noniusprinzip in verschiedensten Spielarten nicht wegzudenken und je nach genauer Anwendung unterschiedlich sicherheitswirksam. Es findet sich auch in Lenkwinkel- oder Lenkmomentsensoren anderer Technologien und vieler Hersteller wieder. Das Unternehmen HELLA KGaA Hueck & Co zum Beispiel verwendet das Noniusprinzip zur Ermittlung

[60] Pierre Vernier, 1580–1637

eines absolut ausgegebenen Lenkwinkels aus den 40° und 20° genau messenden Spulensystemen mit auswertenden ASICs eines induktiv messenden Lenkmomentsensors in Kombination mit magnetischer Winkelsensorik (siehe [67] und [68]).

#### 5.3.1.1 Absolutlenkwinkel

Das Noniusprinzip ermöglicht es, aus der Kombination zweier Winkel zwischen 0 und 360° an verschiedenen Drehachsen einen Drehwinkel zu bestimmen, der an einer der Drehachsen oder an einer dritten Drehachse über die 360° hinausgeht. Durch geeignete Auswahl der Übersetzungen zwischen den Drehachsen kann dieser Winkel beispielsweise auf die Erfordernisse eines sich vier bis fünf Mal um die eigene Achse drehenden Lenkrades angepasst werden. Der resultierende Winkel, der aus der Schwebung und Kombination der beiden verschiedenen Messwerte hervorgeht, ist der eigentliche Messwert, der von Interesse ist. Er ist der zu jeder Zeit eindeutige und absolute Winkelwert einer Drehachse, unter Umständen auch über mehrere Drehrunden hinweg und soll ab nun *Absolutwinkel* genannt werden. Er kann zu jeder Zeit statisch, d.h. ohne Historie von Messwerten oder anderen gespeicherten Werten ermittelt werden.

Der Absolutwinkel bezogen auf das Lenkrad im Fahrzeug wird dann Absolutlenkwinkel genannt und geht in der Regel über mehrere Lenkradrunden. Der Absolutlenkwinkel ist von Interesse für Fahrzeugfunktionen, die auf Daten der mechanischen Stellung des Lenkrades oder der gelenkten Räder bei Wiederaufnahme der Fahrt nach elektroenergielosem Zustand angewiesen sind.

#### 5.3.1.2 Lenkwinkeländerungen

Für die meisten Fahrzeugfunktionalitäten bezüglich Lenkung sind jedoch nur die Änderungen des Lenkwinkels während der Fahrt von Interesse. Die Winkelangabe innerhalb einer Runde zwischen 0 und 360 Grad, bezogen auf einen einmalig festgestellten Bezugspunkt, der übrigens nicht die Geradesausfahrt wie beim Absolutlenkwinkel sein muss, soll ab hier *Relativwinkel* und bezüglich Lenkrads *Relativlenkwinkel* genannt werden.

Die sehr sicherheitskritischen Funktionalitäten bezüglich Lenkung im Fahrzeug sind meist auch sehr zeitkritisch[61]. Daher ist über den Relativlenkwinkel hinaus meist die Dynamik dieser Information, also die Änderungen pro Zeiteinheit notwendig. Etliche Funktionalitäten mit strengsten Sicherheitsanforderungen im Fahrzeug müssen „wissen“, wie und wie schnell der Fahrer die Fahrtrichtung ändern möchte bzw. sich die Fahrtrichtung tatsächlich ändert. Deshalb werden Lenkwinkeländerungen oft zu Gradienten (Winkel pro Zeit) umgerechnet. Physikalisch gesehen ist das die Winkelgeschwindigkeit. Bei der Quantisierung

[61] Versuche haben ergeben, dass eine plötzliche Beaufschlagung des Lenkrades von 9° zur Unbeherrschbarkeit des Fahrzeugs führen kann.

ist man auf eine mehr oder minder große Winkelhistorie angewiesen. Je größer diese Historie von Werten ist, desto weniger fallen einzelne Fehlmessungen ins Gewicht und können so schon gewissermaßen ausgefiltert werden. Gemessen und quantisiert wird dazu in Zeitintervallen von 1 bis 10 Millisekunden.

Die Lenkwinkeländerungsgeschwindigkeit ist wegen der bewegten Massen physikalischen Grenzen unterworfen. Sowohl was die Möglichkeiten von Fahrerin oder Fahrer zur schnellen Drehung des Lenkrades, als auch die motorkraftunterstützte oder durch äußere Gegenstände beeinflusste, tatsächliche Fahrtrichtungsänderung angeht, können bestimmte Grenzen der Dynamik nicht überschritten werden. In einem Fahrzeug mit klassischer Lenksäule und mechanisch fest gekoppelter Lenkübersetzung kann man von maximal 30° am Lenkrad pro Sekunde ausgehen, zum Beispiel bei der schrägen Fahrt gegen einen Bordstein. Höhere Gradienten können ausgeschlossen und daher zur Fehlererkennung herangezogen werden[62]. Eine moderne EPS allerdings vermag diesen Wert zu übersteigen. Sie kann eigenständig, im Fehlerfall sogar unbeabsichtigt, für die Lenkenden absolut unbeherrschbare Winkelgradienten hervorrufen. Das gewollte Überschreiten bestimmter Maximalwerte macht fahrzeugsicherheitstechnisch, z.B. für ein elektronisches Stabilitätsprogramm (ESP), keinen Sinn. Es darf und sollte auch hier pauschal als Fehler gewertet werden.

Kleine Richtungsänderungen, auch mit hoher Dynamik, bleiben für die Lenkenden beherrschbar, wenn bestimmte Gesamtbeträge in größeren Zeiteinheiten nicht überschritten werden. Nach einer Fahrversuchsstudie der Firmen Kostal und BMW liegt dieser Betrag bei etwa 9° am Lenkrad pro Sekunde.

### 5.3.2 Mehraufwand für sicherheitsgerichtete, magnetische LWS

Bei einem magnetischen LWS mit Noniusprinzip zur Feststellung der absoluten Lenkradposition werden in aller Regel mindestens zwei Sensorbausteine benötigt. Das Messergebnis ist (leider) auf beide Sensoren in gleicher Weise angewiesen, sodass sich zur Bestimmung des Absolutwinkels keine Redundanz ergibt und damit die erreichbare Sicherheitsintegrität der Messfunktion auf die des dabei schwächsten Gliedes beschränkt ist.

Um die Ausgabe von Absolutwinkeldaten dennoch mit höherer funktionaler Sicherheit (> ASIL B) zu ermöglichen, muss zusätzliche, redundante Sensorik, eingesetzt werden. Diese sollte natürlich so einfach und rudimentär wie möglich gehalten werden. Beispielsweise nach dem Muster eines Patents [69] kann zu diesem Zweck neben den zwei üblichen Sensoren für das Noniusprinzip zusätzlich ein kleiner Taster eingesetzt werden, der redundant Aufschluss über die momentane Stellung einer Achse geben kann. Auch die Einführung

[62] Dies ist in aller Regel auch üblich.

eines oder zweier zusätzlicher Messräder mit jeweils eigenem Übersetzungsverhältnis nach Abbildung 5.3 (3- oder 4-fach Nonius) bringt eine Redundanz ins Spiel, die, abgesehen von allem Aufwand und damit verbunden erhöhten Gesamtausfallraten, höchst sicherheitsintegere Absolutwinkelausgaben ermöglichte. Flaschenhals für höchste Integrität (ASIL D) bliebe jedoch das oder blieben die dann notwendigen zwei Rechnersysteme zur Datenverarbeitung. Andere, realistischere Konzepte verwenden zur Integritätssteigerung für Absolutwerte mehrere LWS an ganz verschiedenen Einbauorten[63], möglicherweise auch mit verschiedenen Technologien. Beides sind Faktoren, die der funktionalen Sicherheit zur Vermeidung abhängiger Fehler zuträglich sind. Nachteil neben dem Aufwand für Entwicklung und Material ist aber, dass die höhere Sicherheit der Messergebnisse nicht sensorimmanent ist, also nicht bereits mit der Ausgabe der absoluten Lenkwinkel definiert bzw. erreicht werden kann. Die beiden Messwerte müssen erst noch an dritter Stelle miteinander verglichen oder plausibilisiert werden. Der Vergleich selbst muss wieder die für den Absolutlenkwinkel angestrebte Sicherheitsintegrität aufweisen, was für einen ASIL > ASIL B mitunter auch wieder den Einsatz von weiterer Redundanz bedeutet.

Da Absolutlenkwinkel im Fahrzeug, wie in den Abschnitten 5.3.1.1 und 5.3.1.2 erläutert, bislang[64] nicht auf Sicherheitsniveaus höher als ASIL B gebraucht werden, können die beiden für das Noniusprinzip notwendigen Sensoren ausreichen, wenn sie selbst beide mindestens ASIL B erreichen. Nachteilig an den bekannten, das Noniusprinzip verwendenden Lenkwinkelmessvorrichtungen ist jedoch, dass sie zwei Sensoren an verschiedenen Anbauorten erfordern, was zu mehr Platzbedarf und Mehrkosten führt. Mit den Patentanmeldungen im Jahr 2010 [70] und im Jahr 2012 [71] werden Vorrichtungen vorgestellt, bei der die maximal üblichen fünf Runden von Lenkrädern in Kraftfahrzeugen derart abgebildet werden, dass absolute Winkel mit einem einzigen Sensorbaustein eindeutig und dabei mindestens auf der Sicherheitsanforderungsstufe ASIL B ausreichend sicher gemessen und ausgegeben werden können. Bei diesen Lösungen wird ein Hallsensor eingesetzt, der ein Magnetfeld in allen 3 Dimensionen erfasst. So kann der Kostenaufwand beschränkt und gleichzeitig noch eine sensorimmanente Sicherheitsintegrität von ASIL B für die Ausgabe eines Absolutwinkels erreicht werden.

Für Relativlenkwinkel und ihre sicherheitsbezogene Ausgabe stellt sich die Sache für LWS einfacher dar. Grundsätzlich reicht ein einziger Sensorbaustein technisch zur Messung aus. Genauer gesagt sind für eine Ausgabe immer mindestens zwei Messungen notwendig: Eine Messung zur Aufnahme eines Bezugswerts und dann die Messung neuer

[63] „oben“ am Lenkrad und „unten“ am Lenkgetriebe oder am Motor der EPS
[64] Dies könnte sich im Rahmen hoch- oder vollautomatisierten Fahrens eventuell ändern.

Werte. Die jeweiligen Winkeldifferenzen können als Relativlenkwinkel ausgegeben werden. Der mit den Ausgabewerten verknüpfte ASIL kann maximal so hoch sein wie die bei der Winkelmessung und -bestimmung im Sensor erreichte Stufe der Sicherheitsintegrität.
Für die verschiedenen, lenkwinkelbezogenen Funktionalitäten im Fahrzeug wünscht sich der Entwickler der entsprechenden Sicherheitskonzepte, dass er den Winkelinformationen aus einem LWS denjenigen ASIL zuordnen darf, der zur Weiterverarbeitung der Daten auf gleicher Sicherheitsintegritätsstufe benötigt wird. Dies bedeutet, dass der vielerlei benötigte Relativlenkwinkel in einem Sensormodul auf dem Sicherheitsniveau des winkelabhängigen SZs mit dem höchsten ASIL im Fahrzeug ermittelt werden muss. Ohne redundante Sensorquellen und ohne ein ausgeklügeltes, technisches Sicherheitskonzept für einen solchen LWS können ein ASIL D und die zugehörigen Zielwerte der Sicherheitsmetriken jedoch nicht erreicht werden. Wie bereits angedeutet sind dazu bislang Konzepte mit 2 Sensorbausteinen und in der Regel vor allem mit zwei verschiedenen, unabhängigen Rechnersystemen notwendig. Ein Konzept nach dem Vorbild von EGAS mit nur einem Rechnersystem für ASIL D wurde in diesem Bereich zwar erwogen und manchmal sogar realisiert, kommt aber definitiv an seine sicherheitstechnischen Grenzen.

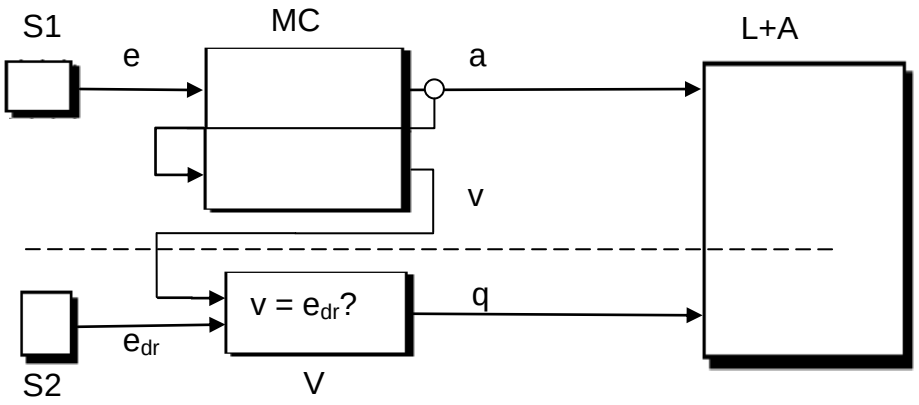
# 6 FUNKTIONELL DIVERSITÄRE REDUNDANZ MIT ASYMMETRISCH ANGEORDNETEM VERGLEICH

In diesem Kapitel wird nun ein technisches Sicherheitskonzept entworfen, das alle vorangehend definierten Anforderungen und Ansprüche erfüllt. Als Konzept für funktionale Sicherheit und zur Entwicklung verschiedenster Systeme im Automobil bietet es lediglich eine grundlegende Sicherheitsarchitektur. Für konkrete Systementwicklungen bietet es in definierten Grenzen viel Freiraum für Variation und Anwendungsflexibilität. Der SM im Konzept basiert auf einem Verfahren [72] zum Vergleich funktioneller Diversität. In Abschnitt 2.7 haben wir gesehen, dass diese bestimmte Art von technischer Diversität sogar Fehler im systematischen Bereich aufzudecken vermag. Genau diese Prinzipien werden an dieser Stelle gezielt dazu eingesetzt, die systematische Integrität eines unter Umständen benötigten SW-Systems so zu erhöhen, dass sein Verifikationsaufwand entsprechend geringer ausfallen darf. Anstatt sich also den aufwändigen Verfahren eines mathematischen Beweises der Richtigkeit eines softwarebasierten Systems zuzuwenden, wird im Weiteren dieser Arbeit untersucht und gezeigt werden, wie ein solches System und insbesondere dessen SW auch konzeptionell technisch und unter Einsatz funktioneller Diversität gegen alle Art Fehler – eben auch im systematischen Bereich – abgesichert wird.
Die Kombination aller in diesem Kapitel genannten Prinzipien und Mechanismen ist so noch nie veröffentlicht worden oder zum Einsatz gekommen (Kapitel 7) und stellt das wissenschaftliche Neuland dieser Arbeit dar, insbesondere, wenn es um die Analyse und Bewertung der funktionalen Sicherheit des so kombinierten Konzepts geht (Kapitel 8).

## 6.1 ASYMMETRISCHE VERTEILUNG DER SICHERHEITSBÜRDE

Für die weitere Entwicklung und Betrachtung eines neuen Konzepts soll nun die Aufmerksamkeit mehr auf die Sensorik und die Eingangsteile des Systems gelegt werden. Für die Steuerung und Ansteuerung im Aktorikteil eines Items soll schlicht von einem ausfallsicherheitsgerichteten Verhalten ausgegangen werden. Einzelne Fehler dort werden das Item hinsichtlich des SZs zunächst nicht in einen unsicheren Zustand führen, auch wenn die beabsichtigte Funktion des Systems nicht mehr gegeben sein sollte. Zur Vermeidung latenter Fehler im Ausgangsteil einer Gesamtfunktionalität werden Diagnosemaßnahmen als SMs wie unter Abschnitt 4.3 beschrieben eingeplant.
In verschiedenen, voran gegangenen Abschnitten wurde bereits deutlich, dass bei ungleich dekomponierten Elementen auf Grund der hohen Anforderungen das einfachere Element stets die größere Sicherheitsbürde (vgl. zugeordneter ASIL) tragen sollte. Im Umkehr-

schluss sollte das redundante Element mit asymmetrisch höherer Sicherheitsverantwortung und -integrität möglichst einfach sein. Hierdurch entsteht ein unterschiedlich aufwändiger Aufbau mit einer Asymmetrie zwischen erstem Kanal und Schutzkanal, die der der aufgeteilten Sicherheitsverantwortung umgekehrt proportional gegenüber steht.
Um also den Schutzkanal so einfach wie möglich und allen Aufwand hierfür gering zu halten, wird eine Art „asymmetrisch zu vergleichende“, funktionelle Diversität angestrebt, bei der die redundante Seite der diversitären Datenverarbeitung und der Fehlerbeherrschung möglichst einfach und für das SZ auf das Notwendigste reduziert gehalten wird. Abbildung 6.1 zeigt das Schema dieser Idee.




S1, S2: Sensoren mit funktionell diversitärer Redundanz und den Signalen e und $e_{dr}$
MC: kombiniertes Rechnersystem (Mikrocontroller)
V: Vergleichseinrichtung; L+A: Leistungstreiber und Aktorik
Abbildung 6.1: System mit asymmetrischem Aufbau in zwei Kanälen

Das insgesamt nur einfach vorhandene Rechnersystem im ersten Kanal oben rechnet das Ausgangssignal a diversitär auf eine mit dem funktionell diversitären Sensorsignal $e_{dr}$ vergleichbare Größe v um. Der Unterschied zum herkömmlichen Ansatz zweier diversitär oder sogar funktionell diversitär arbeitender Rechnersysteme mit parallelen, symmetrischen Prozessen, Vergleichen und Fehlerbeherrschungsmaßnahmen ist, dass das asymmetrisch aufgebaute Schutzsystem im unteren Bereich der Abbildung nun deutlich einfacher aufgebaut werden kann, unter Umständen keine SW mehr benötigt und sich dadurch leichter für höhere Sicherheitsintegrität qualifizieren lässt.

Dieses Prinzip soll in Abschnitt 6.3 anhand des zu Beginn des Kapitels angesprochenen Verfahrens[65] noch konkreter erläutert werden. Grundsätzlich geht es dabei um ein Rechnersystem zur Verarbeitung sicherheitskritische Sensorgrößen mit zwei angeschlossenen Sensoren. Die beiden Sensoren geben diversitär redundante Sensorgrößen aus. Als vierte Komponente kommt bei dem Verfahren ein vom Rechner unabhängiger Vergleicher zum Einsatz. Der Rechner berechnet aus der ersten Sensorgröße mittels einer ersten Funktion eine Ausgangsgröße und aus der Ausgangsgröße mittels einer zweiten, entgegen gerichteten Funktion eine Vergleichsgröße. Am Eingang des Vergleichers liegen diese Vergleichsgröße und die zweite Sensorgröße an. Die zweite Sensorgröße ist dabei keine Eingangsgröße des Rechners und unterscheidet sich mit ihrem Wert quantitativ von der ersten Sensorgröße durch die Funktion g. Durch Berechnungen des Rechners und gegebenenfalls des Vergleichers wird aus der berechneten Ausgangsgröße eine erwartete Vergleichsgröße für die zweite Sensorgröße bestimmt und - natürlich im Rahmen von Mess- und Rechenungenauigkeiten - die Übereinstimmung beider Größen durch den Vergleicher überprüft. Abbildung 6.2 zeigt das Prinzip dieses Verfahrens gemäß [72] mit Vergleicher V, den Sensoreingangsgrößen $e_1$ und $e_2$ sowie dem (softwareunterstützten) Rechnersystem MC und der umgerechneten Vergleichsgröße v.

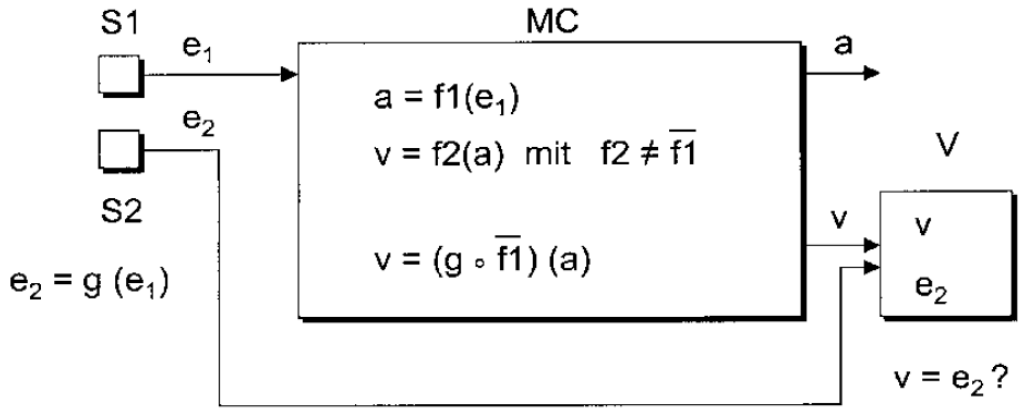



Abbildung 6.2: Prinzip des asymmetrischen Vergleichs gemäß [72]

Bei sicherheitsgerichteten Vergleichen ist grundsätzlich immer auch der Vergleich von Differenzwerten in Erwägung zu ziehen. Differenzwerte zu zwischengespeicherten Vorgängerwerten sind je nach Dynamik der aufgenommenen Größen bedeutend kleiner als die maximal möglichen Werte im definierten Wertebereich. Insbesondere in Fällen, für die die

[65] Siehe Patentschrift DE102008003515 [72] sowie international auch EP2229609, CN101910959, WO2009087187, US8340938, ES2392749

berechneten Differenzen wie für einen Lenkwinkel einen Höchstwert weit unten im gesamten Messbereich physikalisch nicht überschreiten können, kann ein Vergleich entweder mit hoher Auflösung oder einfach mit kleinen Werten durchgeführt werden. Konzeptionell ist jedoch bei diesem Ansatz zu bedenken, dass auch die zweite Sensorgröße vor dem Vergleich auf eine Differenz umgerechnet werden muss, was die vom Rechner isolierte Vergleichseinrichtung V aufwändiger macht und außerdem die Zwischenspeicherung von Werten im Rechnersystem MC und in V erfordert. Aus diesem Grund und wegen der als Muster angestrebten Konzeptdarstellungsform soll diese Möglichkeit im Weiteren der Arbeit nicht weiter verfolgt werden.

Möglicherweise unterschiedlich genau messende Sensoren S1 und S2 bzw. gezielt unterschiedliche Auflösungen in e und $e_{dr}$ können sich ebenfalls sicherheitstechnisch positiv auswirken (erweiterte Diversität) und eventuell sogar zur Kostenoptimierung beitragen. Wegen der Abhängigkeit und Vielfalt von den Entwurfs- und Implementierungsmöglichkeiten in einer konkreten Produktentwicklung wird auch dieser Aspekt hier nicht weiter betrachtet. Zur Veranschaulichung und zur Erreichung höchster Sicherheitsintegrität (ASIL D) werden zwei gleiche Sensorbausteine reichen, die sich in ihren Messwerten wenigstens durch eine lineare und umkehrbare Funktion der Form $e_2 = me_1 + b$ voneinander unterscheiden (für Details siehe Abschnitt 6.3 und weitere). Sofern also $m \neq 0$, $m \neq 1$ und $b \neq 0$ ist, ergibt sich bereits eine erfolgversprechend weite, funktionelle Diversität. Genau diese Funktionsform ist außerdem für eine Realisierung leicht zu finden (siehe Kapitel 7) und die dadurch jeweils zu verarbeitenden Sensordaten werden bereits sicher zu jedem Zeitpunkt systematisch verschieden gehalten.

Bei allem Einsatz von Redundanz ist dieses Verfahren auf "fail-safe"-Verhalten ausgerichtet. Es ist nicht möglich und auch nicht die Absicht, mit diesem Verfahren "fail-operational"-Verhalten zu erzielen, zumindest nicht bei voll erhaltbarer Sicherheitsintegrität. Dieser Aspekt führt uns zum folgenden Abschnitt.

## 6.2 NOTLAUFEIGENSCHAFTEN

Bei dem in den Abschnitten 2.7, 2.8 und 6.1 skizzierten System wurde von einem ersten, oberen Kanal und einem unteren Schutz- oder Absicherungskanal mit Vergleichseinrichtung gesprochen. Entwurfsbedingt werden SPFs ausgeschlossen, denn ein einzelner Fehler im oberen oder unteren Kanal sollte stets zum (als sicher definierten) Funktionsabbruch führen. Damit ist also leicht und ohne weiteren Nachweis eine Hardwarearchitekturmetrik SPFM von quasi 100% erreichbar, wenn abhängige Fehler und insbesondere Fehler mit gemeinsamer Ursache mit Sicherheitsrelevanz einmal unbeachtet bleiben dürfen. Aller-

dings gibt es bei jener Anordnung keine Möglichkeiten eines Notlaufs der Aktorfunktion. Der Absicherungskanal mit Vergleich stellt einen sicherheitstechnisch sehr starken Mechanismus dar, durch den in dem bisher dargestelltem Konzept nun jegliche Einzelfehler (MPFs) in einem der beiden diversitären Sensorkanäle wie auch eigene Ausfälle das SZ nicht mehr direkt verletzen und sogar weitgehend erkannt werden können. Die andere Hardwarearchitekturmetrik LFM bezüglich MPFs kann durch diesen SM für die genannten Bereiche also sehr erhöht werden. Dies geschieht im Betrieb sogar „online“ ohne Zeitverzug hinsichtlich Einhaltung jeglicher FTTIs, wie eigentlich nur bei Ausfällen zu beachten wäre, die direkt das Potential zur Verletzung eines SZs hätten. Leider kann per Vergleich nun nicht unterschieden werden, wo der ausfallbedingte Fehler liegt. Dieser muss nicht unbedingt im unteren Referenzkanal oder in der Vergleichseinrichtung selbst liegen. Theoretisch kann der Fehler auch im ersten, oberen Kanal liegen, wegen des Rechnersystems in Abbildung 6.1 sogar mit statistisch höherer Wahrscheinlichkeit.

Aus den genannten Gründen bietet das Konzept in der bisher dargestellten Form im Fehlerfall noch keinerlei Eigenschaften für einen Weiterbetrieb oder eingeschränkten Notlauf. Notlaufeigenschaften werden aber in jedem guten Konzept benötigt, insbesondere dann, wenn Daten verarbeitet werden sollen, die wie Lenkwinkelinformationen für viele verschiedene Funktionalitäten benötigt werden.

Zu diesem Zweck ermöglicht zumindest der erste Kanal die beabsichtigte Funktionalität einschließlich Aktorik eigenständig. Im mit Abbildung 6.1 skizzierten Fall vermag er den Motor über die Leistungstreiberstufe unabhängig und eigenständig anzusteuern. Es entsteht ein autarker Funktionskanal mit seiner eigenen, natürlich limitierten Sicherheitsintegrität, der durch den Schutz- oder Referenzkanal nicht komplett unterbrochen, deaktiviert oder abgeschaltet werden kann. Die Wirkung des Referenzkanals im Fehlerfall wird eventuell auf die Degradation der kritischsten Funktion(en) und auf entsprechende Warnsignale nach außen beschränkt. Andere, betroffene Items mit geringerem Sicherheitsanspruch sind vielleicht gar nicht erst auf den Referenzkanal und sein Vergleichsergebnis angewiesen.

Der starke SM mit Vergleich vermag auch für diesen Fall Ausfälle aufzudecken, die das Potential haben, anhängige SZs zu verletzen. Er verhindert ebenso SPFs, und erfüllt dabei die Einhaltung jedes erforderlichen FTTIs. Nicht zuletzt wegen seiner Unabhängigkeit kann die SPFM des Systems für ein Item entscheidend verbessert werden, auch wie es z.B. für eine Anwendung mit Betrieb auf Stufe ASIL D gefordert ist.

Fällt jedoch die mit diesem Mechanismus eingebrachte Sicherheitsintegrität bei einem Ausfall weg, so sind die verknüpften SZs allein von der verbleibenden Sicherheitsintegrität des Funktionskanals abhängig. Wird für diesen Fall ein Notlauf geplant, muss im Ent-

wurf einerseits dafür gesorgt werden, dass der Funktionskanal die Funktionen in ihrer dann noch zulässigen Form tatsächlich eigenständig und ausreichend fortführen kann. Dies bedeutet auch, dass das Vergleichselement den Integritätsverlust nur entsprechend anzeigt und diese Funktionen nicht (gänzlich) unterbindet. Andererseits muss der Funktionskanal eine in sich dafür noch jeweils ausreichende Sicherheitsintegrität mitbringen. Diese wird sicherlich nicht mehr höchsten Ansprüchen genügen. Sie reicht jedoch für bestimmte Items und Funktionalitäten oder für eingeschränkte Funktionalitäten mit Warnsignal an die personelle Umgebung des Systems aus. Je nach Sicherheitsintegrität, die als Minimum für alle anhängigen Funktionalitäten und SZs hinsichtlich regulärem Betrieb oder Notlauf benötigt wird, wird der Funktionskanal zu diesem Zweck im entsprechenden, konkreten TSK mit eigenen SMs ausgestattet. Für den Betrieb einer ASIL B behafteten Funktion sind beispielsweise interne Diagnosen wie RAM-, ROM-, und CPU-Tests oder auch die doppelte, inverse Ablage von sicherheitsrelevanten Variablen üblich. Die einzelnen, erforderlichen Maßnahmen werden im Rahmen einer FMEDA deutlich bzw. dort definiert.

Diese SMs im Funktionskanal dienen im Normalfall, also ohne Verlust der Integrität des Schutzkanals, zur Beherrschung von MPFs, zur Vermeidung latenter Fehler und somit zur Verbesserung der Hardwarearchitekturmetrik LFM. Für einen Notlauf oder für den Betrieb von Funktionalitäten mit geringeren Integritätsansprüchen ohne Schutzkanal ist zu beachten, dass die im Funktionskanal integrierten SMs dann statt LFs nun SPF vermeiden müssen und die jeweiligen FTTIs und alle anderen zeitlichen Vorgaben weiterhin einzuhalten sind. Es müssen also ohne Einbeziehung des Referenzkanals die für den geringeren ASIL des Funktionskanals empfohlenen Zielwerte[66] für SPFM, LFM und auch PMHF erreicht werden.

## 6.3 Das Basisprinzip für das neues Konzept

Das Grundprinzip[67] der asymmetrisch angeordneten Vergleichseinrichtung (AAV) soll in diesem Abschnitt näher erläutert werden. Zum Stand der Technik muss zunächst noch Folgendes vorweg genommen werden.

Bei maximal kritisch eingestuften Funktionalitäten im Kraftfahrzeug wurden zur Absicherung gegen Rechenfehler Sicherheitskonzepte mit zwei verschiedenen Rechnersystemen[68] und Busausgaben realisiert. Eine Lösung mit zwei redundanten Rechnersystemen wird im

[66] Bei ASIL B oder im Notlauf bei ASIL B(D): 90% für SPFM, 60% für LFM und <100 FIT für PMHF
[67] Für ein Verfahren mit diesem Prinzip wurde zuletzt im Jahr 2012 die Patenterteilung erreicht.
[68] In der Regel werden Rechnersysteme durch zu Mikrocontrollern integrierte Bausteine (ICs) realisiert.

Bereich eines Massenmarktes aber schnell als zu teuer erachtet. Das für ASIL D bislang geforderte Zwei-Rechner-System wird generell auch als aufwändig und schwierig angesehen. Die damit verbunden erhöhte Komplexität kann zudem wieder als Nachteil für die Zuverlässigkeit und sogar für die Funktionssicherheit angesehen werden.

Wenn bei Lösungen mit nur einem Rechnersystem nicht ein EGAS-basiertes Konzept schon für ausreichend erachtet wurde, kamen auch Ansätze mit zweifach parallel oder sogar invertierend verlaufenden, mitunter diversitär entworfenen Rechenpfaden zum Einsatz, beispielsweise wie mit der deutschen Patentschrift DE 42 19 457 beschrieben [57]. Dadurch wird die Hardware in den beiden Rechnungen in unterschiedlicher Weise benutzt und die Wahrscheinlichkeit, dass sich ein Fehler der CPU gleich auswirkt, wird deutlich verringert. Die Wahrscheinlichkeit der gleichen Fehlerauswirkung wurde durch Fehlerinjektionsexperimente bereits quantifiziert und die hohe[69] Wirksamkeit hinsichtlich der Funktionssicherheit für diesen lokalen Fehlerbereich validiert. Ein genereller Nachweis allerdings, dass die eine CPU nicht in beiden parallel oder invertierend verlaufenden Rechenwegen gleich falsch rechnet, ist faktisch nicht möglich. Zudem könnten für den Vergleich passende Rechenergebnisse leicht durch programmfehlerbedingtes Kopieren oder Überspringen von Programmschritten entstehen. Für den abschließenden Vergleich der Ergebnisse könnten so plötzlich zwei gleiche, aber falsche Ergebnisse vorliegen (z.B. Null = Null). Auch durch bestimmte Hardwareausfälle könnte die CPU im Einfach-Rechnersystem und auch im Falle von Rechenwegen mit invertierten oder antivalenten Daten z. B. beide Rechenwege auslassen und direkt zwei zueinander passende Werte zum Vergleich miteinander bringen. Bestimmte Fehler der CPU, Fehler im Rechnersystem allgemein, im Programm oder auch außerhalb der Rechnersystemgrenzen könnten nicht rechtzeitig aufgedeckt werden oder bleiben vielleicht gänzlich unentdeckt. Höchste Sicherheitsintegrität gemäß ASIL D für Sicherheitsziele ganzer Items mit den bisherigen Ein-Rechner-Lösungen konnte bislang auch nur eingeschränkt oder nur unter Verwendung zusätzlicher HW erreicht, nachgewiesen und unabhängig bestätigt werden. Es mangelt bei diesen Lösungen eben oft an diversitärer Redundanz, die sich ausreichend weit über das System bzw. Item erstreckt und/oder an der Unabhängigkeit der vorhandenen Redundanz bzw. der eingesetzten SMs. Oft ist wie bei EGAS auch keine rechtzeitige Fehleraufdeckung im Rahmen von gesetzten Fehlertoleranzzeitintervallen möglich.

Die für die Automobilindustrie heute gültige Sicherheitsnorm ISO 26262 war zur Zeit der Erfindung des in dieser Arbeit genutzten Vergleichsprinzips noch nicht veröffentlicht. Die daher allgemein anzuwendende Sicherheitsnorm war die IEC 61508. Bestimmte hardware-

[69] hoch im Sinne der Sicherheitsnormen mit niedrig (> 60% DC), mittel (> 90% DC) und hoch (> 99% DC)

technische Mindestwerte, z. B. die für die Metriken PFH (en: probability of safety related failure on high demand) und SFF (en: safe failure fraction) können auch hier in der Regel nur durch zusätzliche Maßnahmen zur Fehlerbeherrschung erreicht werden. Diese wurden und werden aber in der Automobilbranche nach allen Möglichkeiten in SW realisiert. Ein mit ASIL D vergleichbares Restrisiko wird in der IEC 61508 mit dem Sicherheitsintegritätslevel 3 (SIL3) beschrieben. Die heute mit der Sicherheitsmetrik PMHF der Automobilnorm vergleichbare Metrik PFH der IEC 61508 hat allerdings generell um den Faktor 10 niedrigere Zielwerte, z.B. maximal 100 FIT statt 10 FIT für eine Sicherheitsfunktion bei SIL3 bzw. ASIL D. Dies bedeutet, dass zur Minderung eines vergleichbaren Restrisikos bei Anwendung der Automobilnorm eine deutlich höhere Sicherheitsintegrität erreicht werden muss.

Ein Ziel bei der Erfindung des Grundprinzips war es, ein Einfach-Rechnersystem zur Auswertung und Ausgabe sicherheitsrelevanter Sensorgrößen zu schaffen, mit dem eine besonders hohe Sicherheitsintegrität für die Gesamtfunktionalität erreicht wird, ohne z.B. auf einen separaten, aufwändigen CPU-Test angewiesen zu sein.

Als Anordnung ist demnach ein Einfach-Rechnersystem mit wenigstens zwei Sensoren vorgesehen, die bei einem zu erfassenden Systemzustand in ihrer Qualität verschiedene Sensorgrößen oder zumindest jeweils verschiedene Werte ausgeben. Zwischen den stets verschiedenen Ausgangswerten beider Sensoren wird ein bekannter funktioneller Zusammenhang vorausgesetzt. Die Sensorgröße des ersten Sensors am Eingang des Rechners wird dazu genutzt, eine Ausgangsgröße zu berechnen, die für praktisch nutzbare Zwecke, beispielsweise als Steuerungsgröße für ein Stellglied, zur Verfügung steht. Die im zweiten Schritt daraus errechnete Vergleichsgröße entspricht qualitativ und quantitativ der erwarteten Sensorgröße des zweiten Sensors. Diese Vergleichsgröße wird von dem Rechner an eine externe Einrichtung gegeben, die die Vergleichsgröße mit der dem Rechner völlig unbekannten, tatsächlichen Sensorgröße des zweiten Sensors auf Übereinstimmung[70] vergleicht. Ein positives Vergleichsergebnis spricht dabei für die Sicherheitsintegrität des Rechners mit seiner CPU und für eine korrekt abgelaufene Berechnung der Ausgangsgröße. Diese Aussage soll im nächsten Abschnitt 6.4 genauer beleuchtet werden.

Zur weiteren Beschreibung des Verfahrens wird im Folgenden die Bezugszeichenliste zu Referenzzwecken wiedergegeben.

[70] Bei den Begriffen "Vergleich" und "Übereinstimmung" in dieser Arbeit geht es stets um die Prüfung, dass die verglichenen Werte entsprechend den Messabweichungen fehlerfreier Sensoren und auch entsprechend den, wenn auch niedriger erwarteten, Rechenungenauigkeiten einer fehlerfreien CPU nahe beieinander liegen.

Bezugszeichenliste

| | |
|---|---|
| **MC** | Rechner (Mikrocontroller) |
| **S1, S2** | Sensoren |
| **V** | Vergleicher |
| **a** | Ausgangsgröße |
| **e, $e_R$, $e_1$, $e_2$** | Sensorgrößen |
| **e'** | Vergleichsgröße |
| **f1, f2, g, h** | Funktionen |
| **f1** | inverse Funktion (zur Funktion f1) |
| **v** | Vergleichsgröße |
| **$v_1$** | erste Vergleichsgröße |
| **$v_2$** | zweite Vergleichsgröße |

Die grundlegende Voraussetzung der Idee ist natürlich eine sich über weite Teile des Systems erstreckende, funktionelle Diversität, die sich durch qualitativ oder auch nur quantitativ verschiedene Sensoren als den Datenquellen im Signalpfad eines Systems ergibt. Die Sensoren liefern unterschiedliche Messgrößen oder zumindest durch eine Linearfunktion so deutlich unterschiedliche Werte, sodass sie damit während der Verarbeitung und ungeachtet von Mess- und Rechenungenauigkeiten zu jeder Zeit stets für ausreichend unterschiedliche Daten im Speicher des Rechners sorgen. Auch der dabei verwendete Algorithmus (parallel / umkehrend / invertierend / invers / komplementär / antivalent / entgegen gerichtet / zurückrechnend) soll hierbei zunächst keine Rolle spielen.
Zu keiner Zeit ist der fehlerfreie oder fehlerhafte Rechner in der Lage, die zum positiven Vergleich erwartete Größe anders, z. B. durch bloße Kopie der ersten Sensorgröße, zu ermitteln und einem Vergleicher zuzuführen, als durch das Ergebnis einer korrekt abgelaufenen Berechnung. Zum Nachweis der Sicherheitsintegrität des Rechners ist nun ein Vergleich der Vergleichsgröße mit der zweiten Sensorgröße von entscheidender Bedeutung. Verglichen werden die Vergleichsgröße des Rechners und der dem Rechnersystem bisher unbekannte Wert einer zusätzlichen, unabhängigen Datenquelle. Dieser Wert ist durch die zweite Sensorgröße gegeben. Da diese nur außerhalb des Rechners, von seiner CPU ungelesen und unverarbeitet vorliegt, liefert der Vergleich an dieser Stelle ein Ergebnis, das vor allem von der CPU-Integrität des Rechnersystems (Mikrocontroller) abhängt. Vorteil gegenüber diversitären Rechenpfaden, mit denen aus den diversitären Messdaten die gemeinsame Ausgangsgröße a berechnet wird, um anschließend unabhängig extern verglichen zu werden, ist bei der neuen Lösung, dass neben dem Vergleich auch die zweite Vergleichsgröße unabhängig von MC ist und damit die Grenze zwischen diversitären Daten nicht mehr innerhalb von MC liegt. Die Integrität von MC kann durch den Vergleich nun komplett extern überprüft werden. Von Interesse und im nächsten Abschnitt zu untersu-

chen ist nun nur, mit welcher Wahrscheinlichkeit einzelne Ausfälle in MC dazu führen können, dass die Ausgangsgröße a falsch berechnet und die daraus weiter berechnete Vergleichsgröße v wieder derart korrigiert wird, sodass sie zufällig die Messgröße des zweiten Sensors trifft.

Ein stimmiges Vergleichsergebnis kommt aber natürlich auch nur dann zustande, wenn beide Sensoren fehlerfrei arbeiten.

Bei einem ähnlichen Verfahren [57], allerdings schon aus dem Jahr 1992 bekannt, wird ein Ein-Chip-Rechenbaustein dargestellt, also ein Mikrocomputer oder Mikrocontroller, der im Folgenden ebenfalls kurz als Rechner (MC) bezeichnet wird. MC erhält dort die Sensorgrößen (e, $e_R$) von zwei Sensoren (S1, S2) zugeführt. Die Sensorgrößen (e, $e_R$) werden hier als digitale Werte vorausgesetzt, wobei die Sensoren (S1, S2) aber prinzipiell auch analoge Signale liefern können, die innerhalb des Rechners MC digitalisiert werden.

Aus der Sensorgröße e des ersten Sensors S1 berechnet der Rechner MC mittels einer Funktion f1 eine Ausgangsgröße a, die an einem Ausgang des Rechners MC ausgegeben wird, und beispielsweise zur Steuerung eines nichtdargestellten Stellglieds verwendet werden kann. In einem weiteren Schritt berechnet der Rechner MC mittels einer Funktion f2 aus der Ausgangsgröße a eine Vergleichsgröße e'. Da bei diesem Verfahren gemäß DE 42 19 457 [57] die Funktion f2 als die bezüglich der ersten Eingangsgröße e invertierte Funktion $\overline{f1}$ zur ersten Funktion f1 beschreibt, ergibt sich, bei korrekter Funktion des Rechners MC, eine Vergleichsgröße e', die mit der ursprünglichen Eingangsgröße e des ersten Sensors S1 übereinstimmt. Dies kann rechnerintern durch Vergleich (Ist e = e' ?) der Größen e und e' überprüft werden. Mit weiterem Anspruch wird eine Überprüfung der ersten und der zweiten Sensorgröße auf Übereinstimmung (Ist e = $e_R$ ?) vorgeschlagen. Somit wird vorausgesetzt, dass die als redundant bezeichneten Sensoren (S1, S2) quantitativ gleichartige Sensorgrößen (e, $e_R$) ausgeben.

Da ein nicht korrekt funktionierender Rechner MC prinzipiell auch falsche Vergleiche liefern kann, ist darüber hinaus ein, bezüglich des Rechners MC, externer Vergleicher V vorgesehen. Dieser Vergleicher V vergleicht die Sensorgröße $e_R$ des zweiten Sensors S2 mit der berechneten Vergleichsgröße e'. Wegen der oben vorausgesetzten Gleichheit (e = $e_R$ und e = e') muss auch dieser Vergleich, bei korrekt funktionierenden Sensoren (S1, S2) und einem fehlerfrei arbeitenden Rechner MC, Werte der verglichenen Größen (e', $e_R$) bestätigen, die - wieder im Rahmen von Mess- und Rechenungenauigkeiten - übereinstimmen.

Problematisch bei diesem Verfahren ist, dass hierbei bestimmte Fehler des Rechnersystems verborgen bleiben. Ebenfalls ergibt sich ein Problem, wenn die erste Sensorgröße e,

ohne dass eine Berechnung durchgeführt wurde, als vermeintlich berechnete Vergleichsgröße e' an den Ausgang des Rechners MC gelangt. Dies kann beispielsweise dadurch geschehen, dass die erste Sensorgröße e in ein Register des Rechners MC eingelesen wird, und aus diesem Register zu einem späteren Zeitpunkt als vermeintlich berechnete Sensorgröße e' ausgelesen wird und an den Ausgang des Rechners MC gegeben wird, ohne dass tatsächlich eine Berechnung mittels der Funktionen f1 und $\overline{f1}$ stattgefunden hat.
Da die beiden Sensorgrößen e und $e_R$ bereits eingangsseitig wertgleich vorgesehen sind, liefert somit der vom Vergleicher V durchgeführte Vergleich von e' und $e_R$ nun ebenfalls eine Übereinstimmung. Der Vergleicher V ist somit nicht in der Lage, den beschriebenen Fehler aufzudecken.
Ein anderes Szenario, welches zum gleichen fehlerhaften Ergebnis führt, ist dadurch gegeben, dass der Rechner MC sowohl bei der Berechnung der Funktion f1 als auch bei der Berechnung der Funktion $\overline{f1}$ jeweils einen Fehler macht, und sich diese Fehler gegenseitig aufheben. Auch hier können weder rechnerinterne noch rechnerexterne Vergleiche den vorliegenden Fehler erkennen.
Als Beispiel hierfür sei ein systematisch auftretender Vorzeichenfehler genannt, der sich nach zwei fehlerhaften Rechenschritten wieder aufhebt. Dabei bleibt die durch den ersten Rechenschritt berechnete Ausgangsgröße a aber weiterhin fehlerhaft, was sich letztlich gefährlich auswirken könnte.
Diese Fehlermöglichkeiten werden durch das Prinzip im neuen Verfahren ausgeschlossen. Bedeutsam ist zunächst, dass die Sensoren (S1, S2) zwar redundante Sensorgrößen ($e_1$, $e_2$) ausgeben, d. h. unabhängige Signale, die bezüglich des zu erfassenden Systemzustands einen gleichartigen Informationsgehalt aufweisen, deren Signalwerte sich aber wenigstens durch eine oben schon angesprochene, umkehrbare Linearfunktion unterscheiden. Die Sensorgrößen ($e_1$, $e_2$) der Sensoren S1 und S2 stehen demnach in einem bekannten funktionellen Zusammenhang, der durch eine mathematische Funktion g ausgedrückt werden kann. Diese Funktion g sollte einerseits und im Hinblick auf die Verifikation so einfach wie möglich sein. Andererseits soll sie dazu geeignet sein, im Rahmen möglicher Mess- und Rechenungenauigkeiten für ausreichend unterschiedliche Datenniveaus zwischen $e_1$ und v zu sorgen. Verminderte Diversität und damit zu geringe Abweichungen oder gar die Identitätsfunktion könnten wiederum zu den bereits geschilderten Problemen führen.
Für die Praxis soll als Mindestvoraussetzung ein linearer Zusammenhang mit Steigung k und Offset K angenommen werden, für den sich die gemessenen Sensorwerte im gesamten

Messbereich stetig gleichverteilt[71] unterscheiden. Eine Mindestabweichung darf nicht zugesagt werden, da zufällig auch Wertgleichheit der Ergebnisse bestehen kann. Natürlich wäre auch ein komplexerer, aber jedenfalls umkehrbarer Funktionszusammenhang (bijektive Relation) für sehr unterschiedliche Messgrößen und mit größeren durchschnittlichen Unterschieden zwischen den jeweiligen Messwerten zur erfolgreichen Anwendung des Konzepts geeignet und möglich.
Zudem ist die zweite Sensorgröße $e_2$ nur für einen externen Vergleich vorgesehen und wird daher nicht an den Rechner MC gegeben. Sie muss diesem verborgen bleiben.
Eine dritte Bedingung für das neue Prinzip ist, dass die Funktion f2 zur Berechnung der Vergleichsgröße e' bzw. v nicht die invertierte Funktion zur ersten Funktion f1 sein darf, sondern den funktionellen Zusammenhang g zwischen der ersten und der zweiten Sensorgröße ($e_1$, $e_2$) berücksichtigt. Die Funktion f2 ergibt sich damit als Verkettung der zu f1 invertierten Funktion $\overline{f1}$ mit der Funktion g:

$$v = f2\,(a) = (g \circ \overline{f1})\,(a)$$

Bei korrekt verlaufender Berechnung stimmt der am Ausgang vorliegende Wert v mit dem zweiten Sensorwert $e_2$ überein, was durch den Vergleicher V überprüft (Ist $v = e_2$ ?) wird.
Die zuvor für das alte Verfahren beschriebenen Fehlerszenarien sind ausgeschlossen, da die zweite Sensorgröße $e_2$ an keiner Stelle der Berechnung als Eingabewert vorliegt und sich somit nur als Ergebnis einer korrekt abgelaufenen Berechnung oder nur hinreichend unwahrscheinlich zufällig ergeben kann.
Der funktionelle Zusammenhang g zwischen den Sensorgrößen ($e_1$, $e_2$) der beiden Sensoren (S1, S2) kann zunächst durch eine additive Konstante K gegeben sein:

$$e_2 = e_1 + K.$$

So kann beispielsweise vorgesehen sein, dass bei Winkelsensoren der zweite Sensor (S2) einen konstanten Winkelversatz gegenüber dem ersten Sensor (S1) aufweist.
Zur weiteren Diversität, auch im Hinblick auf konstante Offsetfehler, ist zudem damit kombiniert vorgesehen, dass die zweite Sensorgröße $e_2$ ein Vielfaches $k \notin \mathbb{N}$ der ersten Sensorgröße $e_1$ ist:

$$e_2 = k\, e_1 + K.$$

[71] Hinsichtlich des Einsatzes in Kapitel 7 ergibt sich bei je einem Messbereich von $[0..2^{14}\text{-}1]$ der Erwartungswert und Median von $2^{13}$-0,5 und eine Standardabweichung $\sigma_x$ von etwa 4729 ($\sigma_x = (2^{14} - 1)/2\sqrt{3}$ ).

Selbstverständlich könnte in der Realisierung eines konzeptbasierten Systems auch ein weitaus komplexerer Zusammenhang zwischen den Sensorgrößen ($e_1$, $e_2$) bestehen. Insbesondere beim Einsatz zweier Sensoren, die die Sensorgrößen nach unterschiedlichen physikalischen Messprinzipien ermitteln, ergeben sich von vornherein mehr oder weniger komplexe, und damit sicherheitstechnisch grundsätzlich zu vermeidende Zusammenhänge zwischen den Sensorgrößen ($e_1$, $e_2$). Wichtig bleibt jedoch der bijektive Charakter der Relation, d.h. ihre grundsätzliche Umkehrbarkeit.

Bei dem Rechnersystem im neuen Verfahren wird die Sicherheitsintegrität des Vergleichers V am Ende der Verarbeitungskette als gegeben vorausgesetzt. Ein korrekt arbeitender Vergleich bzw. ein korrektes Vergleichsergebnis ist separat zu verifizieren und nachzuweisen.

Für eine Verbesserung an diesem Punkt lässt sich der funktionelle Zusammenhang zwischen der ersten und der zweiten Sensorgröße ($e_1$, $e_2$) durch eine Verkettung von zwei Funktionen h und g darstellen, so dass gilt: $e_2 = (h \circ g)\ (e_1)$.

Innerhalb des Rechners MC wird wieder die bereits beschriebene Berechnung durchgeführt, die hier zu der ersten Vergleichsgröße führt: $v_1 = f2(a) = (g \circ \overline{f1})\ (a)$.

Da aber der funktionelle Zusammenhang zwischen der ersten und der zweiten Sensorgröße hier nicht mehr durch g sondern durch die Verkettung $h \circ g$ gegeben ist, ist die erste Vergleichsgröße $v_1$, die an den Vergleicher V gelangt, nicht geeignet, um mit der zweiten Sensorgröße $e_2$ verglichen zu werden. Der Vergleicher V berechnet daher mittels der Funktion h aus der ersten Vergleichsgröße $v_1$, über die Beziehung $v_2 = h(v_1)$ eine zweite Vergleichsgröße $v_2$, die wegen der folgenden Zusammenhänge bei einer korrekten Funktionsweise des Rechners MC und des Vergleichers V mit der zweiten Sensorgröße $e_2$ übereinstimmen muss.

$$v_2 = h(v_1) = h \circ (g \circ \overline{f1})\ (a) = (h \circ g) \circ \overline{f1}\,(a) = (h \circ g)\ (e_1) = e_2$$

Aus einem positiven Vergleichsergebnis könnte somit geschlossen werden, dass sowohl der Rechner MC als auch sogar der Vergleicher V korrekte Operationen durchführen und die gewünschte HW-Integrität dieser Recheneinheiten damit gegeben ist. Dadurch würde diese verbesserte Ausführungsvariante eine gleichzeitige Funktionsprüfung sowohl des Rechners MC, als auch der Rechenpfade des Vergleichers V ermöglichen.

Auf diese Art der Verbesserung des Konzepts wird aber bei der späteren Konzeptionierung in dieser Arbeit nicht weiter eingegangen, weil die Zielrichtung eine andere ist.

## 6.4 FÄHIGKEIT ZUR ERKENNUNG ALLER ZUFÄLLIGEN EINZELFEHLER IN MC

Ob und warum der zuvor beschriebene Vergleicher tatsächlich alle vorstellbaren, zufälligen Einzelfehler in MC aufzudecken vermag, ist eine der bedeutendsten Fragen im Rahmen dieser Arbeit. Die Antwort darauf wird in diesem Abschnitt erarbeitet. Sie muss eine wissenschaftliche Argumentation bleiben, denn ein Beweis bei einem Bauteil mit vielleicht 3 Millionen Transistoren[72] und jeweils mehreren Ausfallmodi ist nicht vernünftig anzustellen. Aber auch z.B. Fehlerinjektionsexperimente mit echtem oder simuliertem Prozessor, mit denen speziell für den Fehlerbereich MC die gefährlich verbleibende Fehlerrate bzw. die Fehleraufdeckrate DC jenseits der zu übertreffenden 99% statistisch noch genauer quantifiziert werden könnte, sind im Rahmen dieser Arbeit nicht vorgesehen. Da es auch in den einschlägigen Sicherheitsnormen um Risikominimierung, um die Absenkung der Rate[73] für verbleibende, sich gefährlich auswirkende Fehler, und nicht um absoluten Ausschluss aller Risiken geht, stellt sich die oben genannte Frage eher nur nach der Größenordnung des Grads der potentiellen Erkennung in der konzeptbasierten Gesamtanordnung (DC > 60%, DC > 90% oder DC > 99%).
Genauer könnte die Frage oben lauten, ob oder wie nach Abbildung 6.3 ausgeschlossen werden kann, dass ein einziger Ausfall in MC zu einer Verfälschung des Werts a führt, aber der Wert v in Folge wieder korrekt ausgegeben werden kann.

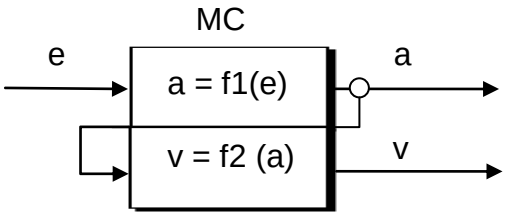



Abbildung 6.3: Rechnersystem MC mit den diversitären Linearfunktionen f1 und f'2

Da ein absoluter Ausschluss aus schon genannten Gründen praktisch unmöglich ist, führt die folgende Frage weiter. Wie hoch ist die Wahrscheinlichkeit P dafür, dass a bei der Berechnung von f1(e) verfälscht wird und v durch die weitere Berechnung von f2(a) durch denselben Ausfall wieder dahingehend korrigiert wird, dass der externe Vergleich zueinander passende Werte feststellen wird? Hält man sich den weit überwiegenden Anteil möglicher Ausfälle in MC vor Augen, der durch den externen Vergleich sicher aufgedeckt

[72] z.B. Renesas µC R8C/34E (R5F2134CWJFP), davon geschätzt 90.000 Transistoren für die CPU
[73] z.B. 146 FIT, davon 4,5 FIT für die CPU im Renesas µC R8C/34E ohne jegliche Maßnahme.

wird, kann man schnell zu dem Schluss kommen, dass allerhöchstens ein Anteil von 1% aller Ausfälle in MC zu dem speziellen, oben in der Frage spezifizierten Fehler führt.
Ohne jede weitere Argumentation kann so festgehalten werden, dass mit $P < 0{,}01$ mindestens schon einmal die Bedingungen der Norm ISO26262 für Sicherheitsmechanismen und den DC für komplexe Bauteile nach ASIL D erfüllt (SPFM $\geq$ 99% bzw. DC $\geq$ 99% bei Failure Rate Class (FRC) 3[74]). Wenn MC den Wert v zum Vergleich korrekt berechnen kann, sollte jedes Zwischenergebnis, also auch der Wert a, mindestens mit $P > 0{,}99$, korrekt sein.
Ein zum kritischen Fehler geeigneter Ausfall in MC müsste also das Zwischenergebnis a verfälschen und das Endergebnis v in weiteren Rechenoperationen wieder korrigieren. Die Wahrscheinlichkeit bei defektem MC für ein verfälschtes Endergebnis v kann ebenfalls leicht als mindestens hundertfach höher angesehen werden, als für die einzig gefährliche Situation eines verfälschten Zwischenergebnisses a mit einem zum Vergleich wieder korrekt getroffenen Wert v. Der jeweils richtige Wert v steht (bei richtiger Implementierung ohne Zwischenspeichern von Werten und mit Setzen von Default-Werten nach jedem Messzyklus) in MC nirgends zur Verfügung und kann also nicht irgendwo kopiert werden. Außerdem sind der Zwischenwert a und das davon abhängige Ergebnis v dynamische Werte und können nicht in fehlerbedingten Vorzugslagen passend zueinander gefunden werden.
Ein Beispiel auf der Suche nach möglichen, kritischen und nicht erkennbaren Einzelfehlern könnte vielleicht eine ausfallbedingte Negierung bzw. Multiplikation mit -1 sein. Ein solcher Ausfall könnte den Wert a nach seiner Berechnung fälschlicherweise negiert erscheinen lassen und den Wert v nach ähnlichen Rechenoperationen in MC wieder mit erwartetem Vorzeichen. Welcher Transistor oder welche Transistorgruppe in MC mit insgesamt mehreren Millionen Transistoren für genau diese Situation verantwortlich ist, kann natürlich nicht ohne Weiteres untersucht werden. Die Wahrscheinlichkeit jedoch, dass ausgerechnet dieser kleinste Bereich als erster aller beanspruchten Bereiche unerkannt ausfällt, könnte sogar als vernachlässigbar gering im Sinne von $P < 0{,}1\%$ betrachtet werden (1:1000). Zur Erinnerung führt der Rechenweg von $e_1$ zu a und von dort zu v zwangsläufig an allen 4 Grundrechenarten vorbei und deckt damit weite Transistor-, Gatter, und Registerbereiche der arithmetischen Logikeinheit (ALU) der CPU innerhalb von MC ab. Zur Vorbeugung könnte man speziell für diesen Fall für eine jeweils ungerade verteilte

[74] Die zweite, in der ISO 26262 genannte Methode zur Auswertung möglicher Verletzungen von SZs durch zufällige HW-Ausfälle soll hier nicht angewandt werden, und zwar nicht, weil nicht auch der Nachweis für 99,9% DC für Bauteile bis 100 FIT Basisausfallrate gelingen könnte, sondern weil die der Methode zugrunde liegende Annahme von maximal 100 Bauteilen im konkreten Item für absolut unrealistisch gehalten wird.

Anzahl gleicher Rechenoperationen für f1 und f2 vorsehen, d.h. z.B. ungerade Anzahlen der Assemblerbefehle NEG, MUL usw.

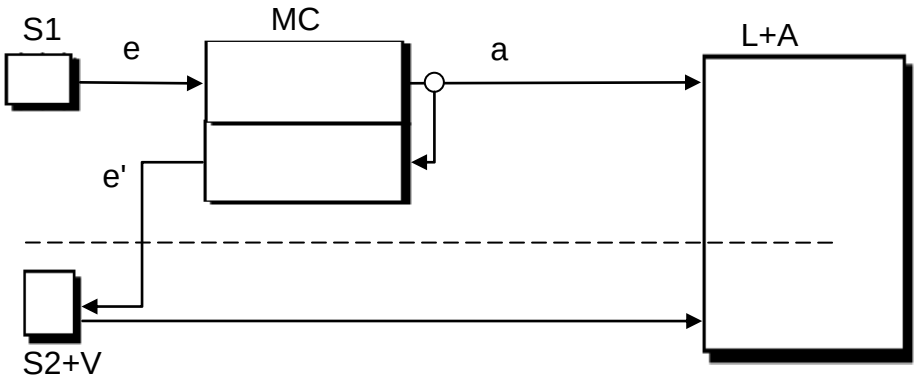
Zwei gleichzeitige Ausfälle an zwei verschiedenen Stellen in MC werden von vornherein ausgeschlossen. Es wird immer von einer ausreichend hohen Erkennungsrate und einer ausreichend schnellen Fehlerreaktion durch den Vergleichsmechanismus für den als erstes auftretenden Ausfall ausgegangen, insbesondere bei Sensorsystemen mit Mess- und Vergleichsfrequenzen bis 1000 Hertz. Zudem bietet die Messwertdynamik wie z.B. bei einem LWS durch kleine Lenkradbewegungen und die dadurch intensiv wechselnden Daten zur Verarbeitung in MC eine zusätzliche Redundanz, sodass der gesuchte Ausfall auch bei verschiedensten Datenniveaus in MC zu seinem gefährlichen Effekt führen müsste.

Voraussetzung dafür, dass sich nicht bei der Ausgabe des Werts a Fehler einschleichen, die durch den Vergleichsmechanismus am Ende nicht aufgedeckt werden können, ist eine Übernahme des Ausgabewertes zur Weiterrechnung an einem Ort, der durch einen weiteren SM im anschließenden Signalpfad ausreichende Integrität (≥ ASIL B) bietet. Zu diesem Zweck muss der Wert a außerhalb von MC aus einem abgesicherten Übertragungskanal zurückgelesen werden. Bei digitaler Übertragung per Bussystem darf auf diesen Wert zur Weiterberechnung auch innerhalb von MC zugegriffen werden, und zwar nach dem Provisionieren und Anlegen einer zur Fehleraufdeckung geeigneten Ende-zu-Ende-Absicherung auf Anwendungsebene (siehe Abschnitte 6.6 und 6.7 für Details).

## 6.5 Weitere Vereinfachung durch Integration

Das im Abschnitt 6.3 beschriebene Basisprinzip soll nun konkret und konsequent für ein neues FSK verwendet werden. Es verspricht schon an sich sicherheitsfördernde Einfachheit und nebenbei die Kosten für ein zweites, diversitär redundantes Rechnersystem (Mikrocontroller, Taktgenerator, Energieversorgung mit Spannungsregler) einsparen zu können. Notwendige Rechen- und Signalanpassungsoperationen werden mit einem einzigen Rechnersystem vorgenommen. Das redundante Referenzsystem zur Absicherung bis hin zur Aktorik eines Systems besteht neben Verbindungsleitungen nur aus einem redundanten Sensorbaustein und einem möglichst einfach gehaltenen Vergleichselement. Eine weitere Vereinfachung kann durch weitere Integration der Bestandteile auf bestehende Bauelemente erreicht werden. Hierzu wird der Referenzsensor S2 und die Vergleichseinrichtung V aus Abbildung 6.1 zu einer integrierten Lösung in einem einzigen Baustein vereint. Beide Elemente in Reihe angeordnet müssen ohnehin gleiche Sicherheitsintegrität bzw. den gleichen ASIL für die Dekomposition zwischen eigentlichem Funktionskanal und

Referenz erreichen. Abgesehen von den Leistungstreibern und dem Rest der Aktorik entsteht so ein Systemkonzept mit nur drei „intelligenten“ Bausteinen bzw. Mikrochips.
Bei der Anwendung des so dargestellten Konzepts wird der elektronisch realisierte Teil einer Gesamtfunktionalität bzw. eines Items komplett in einem Modul auf einer Leiterplatte[75] zusammengefasst, um eine ECU zu bilden. Abbildung 6.4 verdeutlicht diesen Aufbau.
Insgesamt liegt der Fokus des FSKs weniger auf den Bereichen L+A und deren sicherheitstechnischer Beschaltung, sondern im Hinblick auf den konkreten Einsatz zur Lenkwinkelerfassung in Kapitel 7 vor allem auf der Sensorik und dem Logikteil. Trotzdem und zur allgemeinen Anwendung des FSKs könnten auch die Leistungstreiber L und vielleicht auch die Aktorik A in Form eines Relais, eines Summers, einer Signallampe, eines Magnetventils oder eines kleinen Motors (via TSK) auf der selben Leiterplatte integriert sein.
Wichtig bei dieser Art der Integration des gesamten Items in ein Modul ist natürlich zu beachten, dass die Überdeckung des Systems mit funktioneller Diversität bis zur Ausgangsgröße a so weit wie möglich reichen, also so viel Logik wie möglich umfassen soll.
Über die Sicherheitsintegrität für nicht eingeschlossene Logikbereiche rechts hinter a kann zumindest durch den Kernmechanismus des Vergleichs und sein Ergebnis keine Aussage getroffen werden. Idealerweise kann die Aktorik deshalb direkt mit a und ohne weitere Logik angesteuert werden. Die gesamte Logik des Items befindet sich in MC und führt dann zur einzigen Ausgangsgröße a, die zum Vergleich wieder auf eine funktionell diversitäre Sensorgröße zurückgeführt und im entsprechenden Sensorbaustein extern verglichen werden kann.




S1: erster Sensor
S2+V: funktionell diversitärer Sensor mit integrierter Vergleichseinrichtung
MC: kombiniertes Rechnersystem (Mikrocontroller)
L+A: Leistungstreiber und Aktorik
Abbildung 6.4: Weiter vereinfachtes Konzept mit asymmetrischem Aufbau in zwei Kanälen

[75] Leiterplatte (en: printed circuit board, PCB)

Die Verbindung der Blöcke des unteren Abschaltpfads im Konzepts in Abbildung 6.4, bestehend aus S2+V und L+A, kann beispielsweise als ausfallsicherheitsgerichtete Signalleitung realisiert werden. Im Normalfall sorgt diese Leitung dann dafür, dass die Aktorik funktionsfähig bleibt, beispielsweise durch die Freigabe (Aktivierung) eines Leistungstransistors an der Masseanschlussseite eines elektrischen Aktors. Im Fehlerfall, aufgedeckt durch die Vergleichseinrichtung V, wird diese Leitung dann energielos. Dies wiederum führt zur Blockierung (Deaktivierung) des Masseanschlusses des Aktors, zu dessen Funktionsunfähigkeit und damit zur Verhinderung einer möglichen Verletzung definierter SZs.
Für den Fall, dass ein Notlauf vorgesehen ist, wird die genannte Leitung zur Aktorik lediglich zu einer gewissen Degradation des Funktionsumfangs mit Ausschluss der kritischsten Funktionen führen. Vielleicht wird bei einer Realisierung als Fehlerreaktion aber einfach nur die sonst aktiv gehaltene Blockierung einer Warneinrichtung aufgehoben.
Fragen zur sicheren Übertragung von Daten und Signalen werden später in Abschnitt 6.7 und vor allem im konkreten Einsatz des neuen Konzepts (Kapitel 7) wieder aufgegriffen.

## 6.6 Prinzipielle Konzeptanwendung

In diesem Abschnitt soll das Konzept durch die Beschreibung eines konkreten Ablaufs in einem Sensormodul erläutert werden. Die Darstellung wird dazu von einer seriell, digitalen Schnittstelle zwischen den Bausteinen und einem Bussystem zur weiteren Übertragung der sicherheitsgerichteten Sensordaten an verschiedene Empfänger ausgehen. Der Aufbau des Sensormoduls besteht aus einem ersten Sensor 1, einem Mikrocontroller (MC) und einem zweiten Sensor 2, der zudem die Vergleichseinrichtung AAV enthält. Die folgenden sieben Abbildungen stellen den Ablauf in 7 aufeinanderfolgenden Schritten dar.
In Schritt 1 (Abbildung 6.5) gibt der MC zunächst die Messanforderung an die beiden Sensoren aus, damit diese möglichst zeitgleich ihre beiden verschiedenen Messwerte aufnehmen. Dies geschieht vorzugsweise botschaftslos über ein von beiden Sensoren gleichzeitig erkennbares Handshake-Signal (z.B. "chip select", CS). Die Anforderungsrate bei diesem zyklisch wiederkehrenden Prozess muss den engsten, zeitlichen Anforderungen aller abhängigen Funktionalitäten und der für die verschiedenen SZs maximalen Fehlertoleranzzeit angepasst werden. Die Gleichzeitigkeit ist natürlich für die Genauigkeit der Messwerte wichtig, insbesondere bei hoher Änderungsdynamik. Es sollen aber am Ende auch nicht die entsprechend verschiedenen Werte für den Ist-Stand aus verschiedenen Zeitpunkten innerhalb eines Messzyklus verglichen werden. Gänzlich fehlende Messanforderungen im jeweiligen Messzyklus bleiben sicherheitstechnisch hingegen unkritisch,

denn MC kann ohne Messwert aus Sensor 1 nicht fortfahren und auch die AAV in Sensor 2 wird nicht ohne rechtzeitig lesbare Mess- und Vergleichswerte arbeiten.

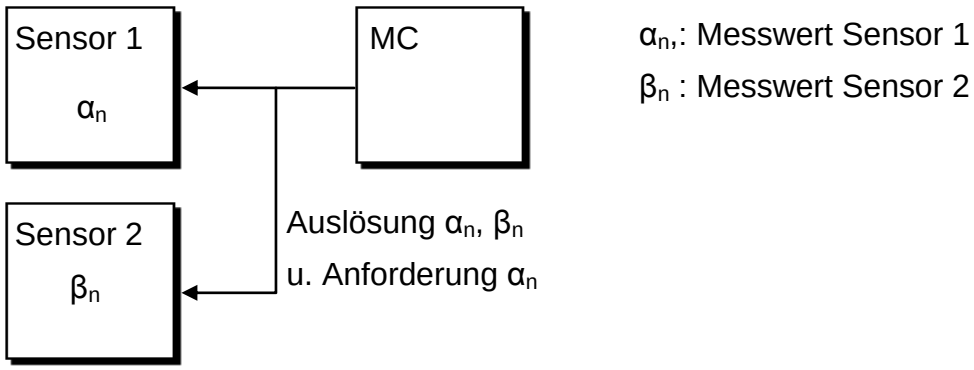



Abbildung 6.5: Asymmetrisch angeordneter Vergleich, Schritt 1

Mit Schritt 2 in Abbildung 6.6 liest MC den gemessenen Wert $\alpha_n$ aus Sensor 1 aus. Die Kommunikation zwischen den Elementen der hier vorgestellten Anordnung geht von digitalen Werten aus und wird als SPI (en: Serial Peripheral Interface) angenommen, wobei MC als Master und die Sensoren als Slaves fungieren. Die in Sensor 2 erfassten Messwerte werden allerdings nicht ausgelesen und sollen MC verborgen bleiben.

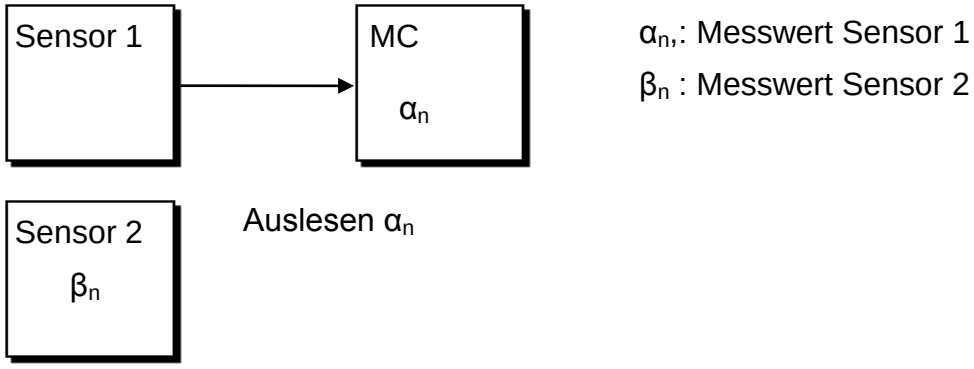



Abbildung 6.6: Asymmetrisch angeordneter Vergleich, Schritt 2

In Schritt 3 errechnet MC aus dem Messwert $\alpha_n$ mittels einer Funktion $f(\alpha_n)$ seinen Ausgabewert Y, beispielsweise einen für die Anwendungen fertig adaptierten Lenkwinkelwert. Für den sofortigen oder auch späteren Versand über ein Bussystem in das ihn verwendende System muss eine ihn enthaltende Botschaft bereits noch auf Anwendungsebene Ende-zu-Ende abgesichert werden. Dazu sichert MC Y durch einen Botschaftszähler BZ und einen Prüfcode CRC, der Y und BZ einbezieht, ab.

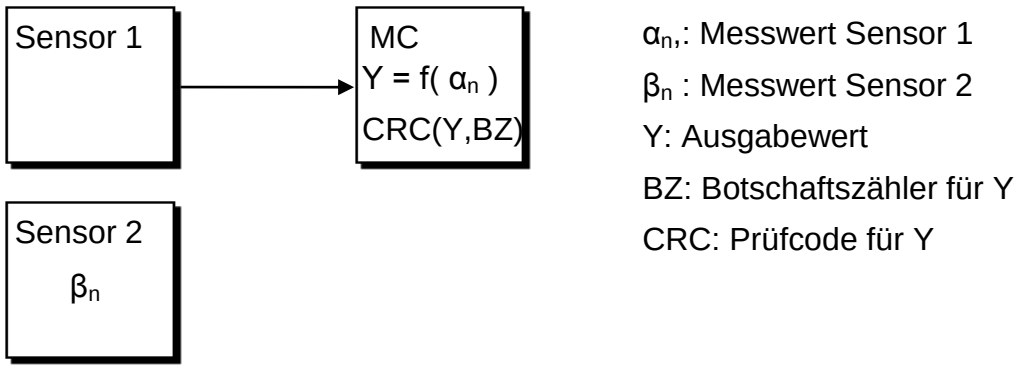



Abbildung 6.7: Asymmetrisch angeordneter Vergleich, Schritt 3

Aus dem zum weiteren Versand abgesicherten Botschaftsrahmen wird der Ausgabewert Y nun wieder zurückgelesen und aus diesem ein Wert ß$_v$ zur Erwartung in Sensor 2 errechnet, wie Schritt 4 in Abbildung 6.8 zeigt. Der Ausgabewert a in Abbildung 6.4 wird hier also nicht erst außerhalb von MC zurückgelesen. Wichtig dabei ist, dass fehlerbedingte Manipulationen von Y nach dem Zurücklesen erkannt werden können, wenn auch durch den anderen Sicherheitsmechanismus der Ende-zu-Ende-Absicherung. An dieser Stelle wird es auf eine saubere Implementierung in MC ankommen, durch die unbeabsichtigte (alte oder erneut erstellte) Botschaften mit falschem Y, aber gleichem Botschaftszähler sicher verhindert wird. Nach jedem Messzyklus müssen dazu z.B. alle Botschaftsrahmen und -daten gelöscht bzw. neu initialisiert werden.
MC überträgt diesen Wert an Sensor 2. Eine Absicherung per CRC und Botschaftszähler ist hierzu nicht notwendig, da jegliche Verfälschungen durch den durch die Übertragung angestoßenen Vergleich in Sensor 2 aufgedeckt werden. Ein Botschaftsidentifier (Id) gegen Maskerade-Fehler ist im Rahmen des Master-Slave-Protokolls von SPI ohnehin nicht notwendig.

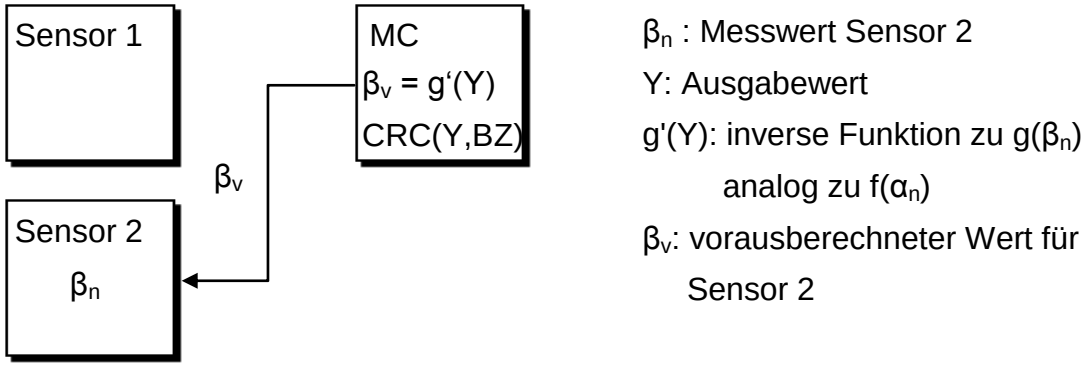



Abbildung 6.8: Asymmetrisch angeordneter Vergleich, Schritt 4

Mit Schritt 5 in Abbildung 6.9 stellt Sensor 2 den Vergleich des vorausberechneten Werts $ß_v$ aus MC mit dem selbst ermittelten, funktionell diversitären Messwert $ß_n$ an. Wegen Mess- und Rechenungenauigkeiten muss dieser Vergleich je nach Quantisierung unter Umständen in einem gewissen Toleranzfenster durchgeführt werden. Bei Übereinstimmung (innerhalb eines vorkonfigurierbaren Toleranzfensters) ist die volle Sicherheitsintegrität des Ausgabewertes Y gegeben. Konzeptionell steht nun die Aufgabe bevor, das Vergleichsergebnis Q den nach außen angeschlossenen Anwendungen in angemessener Integrität zu übermitteln. Bei digital vorgesehener Übertragung ist dazu an dieser Stelle (noch in Sensor 2) und unabhängig vom Medium (SPI, Bussystem oder beides in Kombination mit MC) wieder die Provisionierung einer Ende-zu-Ende-Absicherung vorgesehen. Im Fall der Nichtübereinstimmung (Fehlerfall) liegt eine Einschränkung der Integrität des Ausgabewerts Y vor, die natürlich ebenfalls kommuniziert werden muss. Entweder werden dann die sicherheitstechnisch anspruchsvollsten Funktionalitäten degradiert oder diese Anwendungen komplett abgeschaltet.

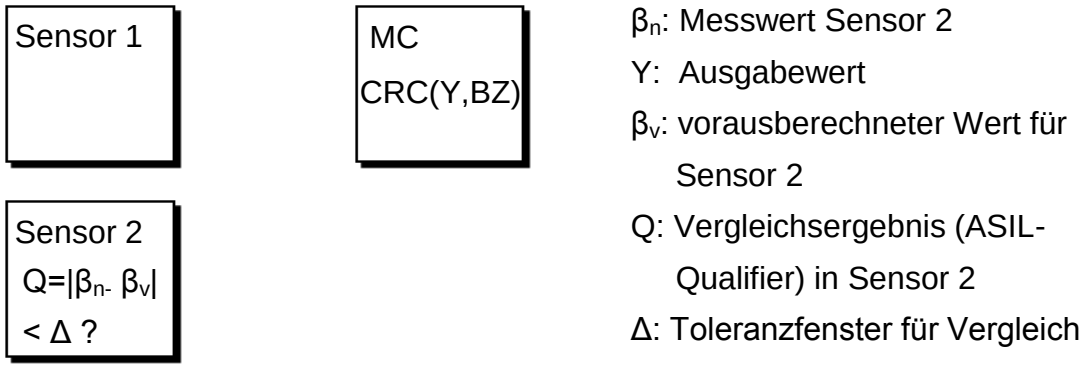



Abbildung 6.9: Asymmetrisch angeordneter Vergleich, Schritt 5

Die Integrität dieser Art Fehlerbeherrschung muss denselben ASIL wie der ganze Mechanismus erreichen. Sofern das Vergleichsergebnis Q nicht direkt durch ein Abschaltsignal per HW, beispielsweise einer Leitung, vermittelt werden soll, sondern oder zusätzlich digital wie der Ausgabewert Y über ein Bussystem, wird es als *ASIL-Qualifier*, der die erreichte Integrität spezifiziert, zur Auswertung an die Aktorik vermittelt. Dieser sechste Schritt kann entweder direkt über eine eigene Bussystemschnittstelle geschehen oder, wie in Abbildung 6.10 gezeigt, getunnelt über MC und seine eigene Bussystemschnittstelle. Die erneute Involvierung von MC im Ende-zu-Ende gesicherten Übertragungsweg bedeutet dabei keinen Nachteil. Denn erstens werden Ressourcen wie z.B. die Kommunikationsschnittstellen von MC wiederverwendet, was den Aufbau vereinfacht, und zweitens wäre bei einem Ausfall von MC jede abhängige Anwendung ohnehin funktionsunfähig (und

natürlich sicher), weil keine Mess- oder Ausgangsgröße mehr ausgegeben werden kann. Ein einziger Wert dieses digitalen Qualifiers steht für volle Integrität, alle anderen Werte zeigen das Gegenteil an. Zur Absicherung der digitalen Übertragung muss das Vergleichsergebnis Q im Sensor 2 noch entsprechend verpackt werden, um die Integrität der Daten wieder bis zur Anwendung im System hin überprüfen zu können. Die Absicherung besteht auch hier aus einem Laufzähler und einem Prüfcode, der als CRC wieder über den gesamten Botschaftsinhalt mit Vergleichsergebnis und Zähler berechnet wird.

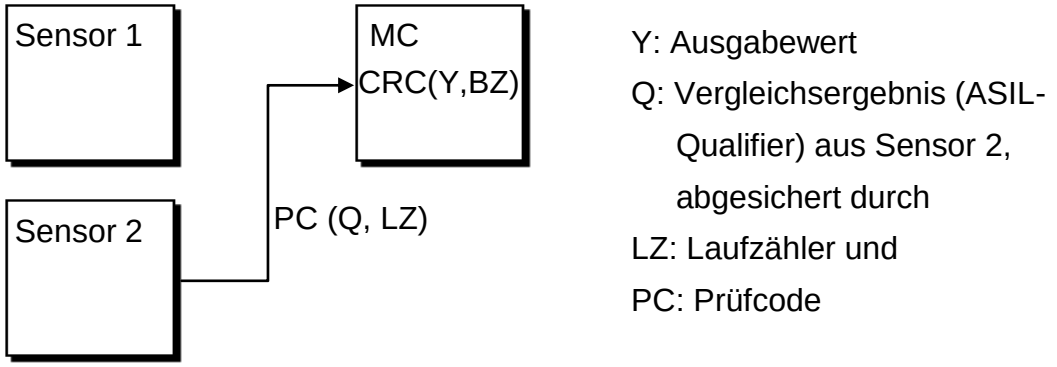



Abbildung 6.10: Asymmetrisch angeordneter Vergleich, Schritt 6

Der letzte Schritt eines Mess- und Absicherungszyklus ist Schritt 7 und durch Abbildung 6.11 verdeutlicht. MC hat die zur Kommunikation bereits fertig abgesicherte Vergleichsinformation bzw. den ASIL-Qualifier Q empfangen und sendet diesen als Botschaft unverändert an eine weitere Logikschaltung oder auch nur an die intelligente Aktorik einer Gesamtfunktionalität, die auf höchste Sicherheitsintegrität angewiesen ist.

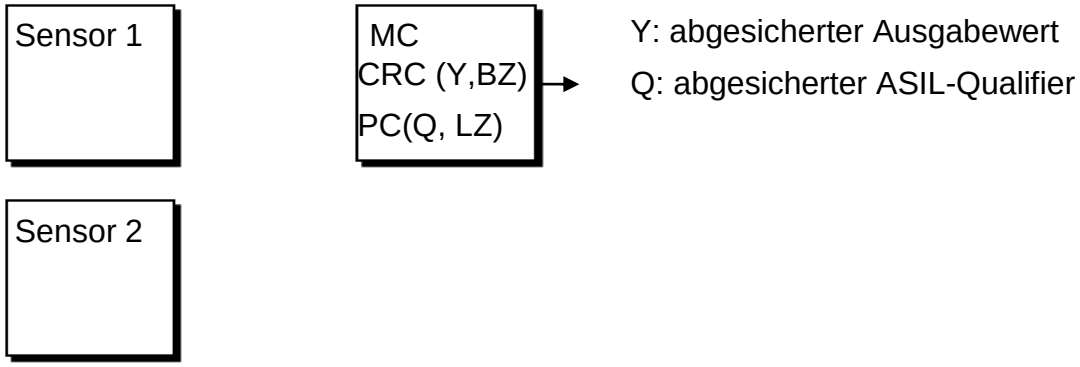



Abbildung 6.11: Asymmetrisch angeordneter Vergleich, Schritt 7

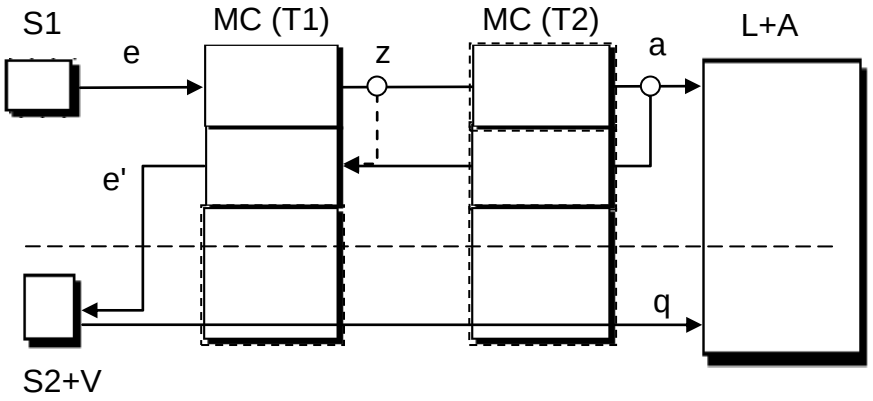
Y und Q können problemlos über den gleichen Bus gesendet werden, wenn eine vollständige Ende-zu-Ende Absicherung besteht. Die beiden Nachrichten müssen allerdings wieder von fehlerunabhängigen Einheiten in elektrische Signale umgesetzt werden. Die Emp-

fängerseite erfordert also (zumindest zum Erhalt höchster Sicherheitsintegrität) wiederum geeignete Redundanz, die aber im Rahmen dieser Arbeit nicht weiter betrachtet und beispielhaft durch den Einsatz verschiedener Einheiten für High-Side und Low-Side nur angedeutet wird.
Vorgesehen ist, dass MC die beiden Botschaften mit Y und Q möglichst zeitgleich an das Bussystem übergibt. Die empfangende Schaltung oder auch Anwendung muss das Eintreffen der beiden Botschaften zeitlich überwachen. Ausbleibende Botschaften oder zeitlich nicht zum eigentlichen Ausgabewert Y passende ASIL-Qualifier werden als Fehler gewertet. Nach Eintreffen einer Botschaft mit seiner richtigen Identifikation werden sodann die jeweils begleitenden Absicherungsinformationen ausgewertet. Zuerst wird überprüft, ob der Prüfcode CRC für Y bzw. PC für Q passt. Danach wird geprüft, dass sich der Botschaftszähler BZ bzw. Laufzähler LZ in der richtigen, erwarteten Reihenfolge befindet. Jeder Fehler bei allen Überprüfungen, selbstverständlich auch ein nicht mit dem für volle Integrität vereinbarten Wert übereinstimmender ASIL-Qualifier, muss dann eine angemessene Fehlerreaktion auslösen. Fehler in der Botschaft mit Q müssen gegebenenfalls zur Fahrerwarnung, zur Degradation des kritischsten Betriebs im Item, zu einer ausreichend sicheren Deaktivierung der Aktorik oder direkt zur Abschaltung der Funktionalität führen.
Der erläuterte, schon konkretere Ablauf wird im folgenden Kapitel 7 von seiner allgemein geltenden Form auf ein magnetbasiertes Lenkwinkelsensormodul übertragen.

## 6.7 Kommunikations- und Datenübertragungswege im Konzept

Vor der Konzeptanwendung in Kapitel 7 sollen in diesem Abschnitt noch die verschieden möglichen Signalpfade im neuen FSK zusammengefasst werden. Zwischen den einzelnen Sicherheitselementen in Abbildung 6.4, hauptsächlich zwischen den eingeplanten, mikroelektronischen Komponenten S1, MC, S2+V und L+A, müssen verschiedenartige Signale und Daten übertragen und kommuniziert werden. Für alle zu übertragenden Daten, ob digital oder als Hardwaresignal vorliegend, muss dafür Sorge getragen werden, dass sie gemäß Sicherheitsarchitektur und angewandter Dekomposition(en) auf einer entsprechenden Sicherheitsintegritätsstufe übermittelt werden können. Zur Verbesserung der Sicherheitsintegrität eines Signals kommen entweder Maßnahmen in TSK oder Entwurf oder aber weitere SMs in Betracht. Grundsätzlich können auch hier die bereits unter Kapitel 4 und insbesondere unter Abschnitt 4.7 genannten SMs oder konzeptionelle Maßnahmen herangezogen werden. Nun lässt das Konzept jedoch viele Freiheiten bei der Ausgestaltung der Art der Signal- und Datenübertragung. Die Pfade an sich bleiben im Konzept jedoch fest vorgegeben, auch wenn ihr Verlauf ebenfalls variieren darf.

Eine Besonderheit für die Architektur der Signalwege stellt der Fall dar, dass sich MC als logische Einheit unter Umständen auch auf zwei oder mehr Rechnersysteme verteilen lässt, die beispielsweise über ein Bussystem miteinander verbunden werden. Diese Konstellation bietet sich vor allem dann an, wenn das Item auch örtlich verteilt ist und die Aktorik nicht am gleichen Ort wie die Sensorik wirken muss. Die in Kapitel 7 beschriebene Konzeptanwendung für ein Lenkwinkelsensormodul mit verschiedenen, abgesetzten Anwendungen ist ein ganz konkretes Beispiel dafür.
Folgende Abbildung 6.12 gibt eine Übersicht der möglichen Signalpfade und einiger Variationen wieder.




S1: erster Sensor
S2+V: funktionell diversitärer Sensor mit integrierter Vergleichseinrichtung
MC(T1+T2): optional verteiltes Rechnersystem mit Teil 1 und optional Teil 2
L+A: Leistungstreiber und Aktorik
Abbildung 6.12: Übersicht möglicher Signalpfade im neuen Sicherheitskonzept

Gestrichelt gezeichnete Blöcke oder Signalwege in dieser Abbildung sind optional. Demnach können die jeweils unteren Bereiche der Teile T1 und T2 von MC entfallen, wenn das Vergleichsergebnis q nicht zum Beispiel als serielle Digitalbotschaft durch einen oder beide dieser Bereiche hindurchgeführt werden soll. Die dann zum Einsatz geplanten Mikrocontroller dienen als Signalumsetzer (Gateways), wobei eine für diesen Fall vorzusehende Ende-zu-Ende-Absicherung zwischendurch natürlich nicht aufgebrochen werden darf. Die auf Anwendungsebene erstellten Botschaften müssen unversehrt bleiben, auch wenn sie zwischendurch in zusätzliche Rahmen verpackt werden.
Alternativ (oder auch - nicht eingezeichnet - zusätzlich) wird q direkt an die Aktorik auf der rechten Seite der Abbildung geführt. Auch hierfür ergeben sich durch verschieden mögliche Technologien mehrere Arten der Signalübertragung. Als digitale Botschaft könnte q seriell an einen Baustein der Leistungstreiberstufe für die Aktorik übertragen

werden. Andere Varianten ergeben sich durch parallele Datenübertragung an einen auswertenden Digitalbaustein im Bereich T+A oder auch ganz einfach durch eine elektrische Signalleitung, die im Fehlerfall ihr Spannungspotential verliert. Diese Leitung wird zur weiteren Absicherung für hohe Sicherheitsintegrität pulsweitenmoduliert (PWM). Nur ein ganz bestimmter Tastgrad steht dann für Übereinstimmung beim asymmetrisch angeordneten Vergleich und führt in der Aktorik nicht zur Einschränkung der Funktionalität.

Der Normalfall des Konzepts ist sicherlich die Variante ohne ein verteiltes Rechnersystem MC, bei dem auf den optionalen Teil T2 verzichtet wird. Ist dies aus oben genannten Gründen nicht möglich, so stellt sich für den Signalpfad der Voraus- bzw. Zurückberechnung von Vergleichsgröße e' die Frage, ob als Basis die Ausgabegröße a oder eine Größe z zwischen den Teilen T1 und T2 des Rechnersystems herangezogen werden soll. Sicherheitstechnisch gesehen ist Ausgabegröße a zu präferieren, denn auf diese Weise erstreckt sich die funktionelle Diversität im Konzept auch über T2, sodass mittels Vergleichseinrichtung auch die Sicherheitsintegrität von T2 überprüft und gewährleistet werden kann. Anders sähe dies aus beim Abgriff der Zwischengröße z, denn dann muss die nötige Sicherheitsintegrität für T2 noch in anderer Weise hergestellt werden.

Unerheblich bei dieser Konstellation ist übrigens, ob die Berechnungen von e nach a und von a nach e' in T1, in T2 oder kreuzweise verteilt in T1 und T2 stattfinden. Fehlt in einem der MCs die eine oder sogar beide Berechnungen, hat der betreffende MC an dieser Stelle nur eine Tunnel- bzw. Gateway-Funktion, deren Fehler durch AVV oder E2E-Sicherung aufgedeckt werden. Eine insgesamt höhere Sicherheitsintegrität kann sich durch die Verteilung der beiden Rechenfunktionen auf unterschiedliche MCs nicht ergeben.

Alle Signalpfade, deren technische Varianten und Möglichkeiten zur Herstellung von Sicherheitsintegrität werden in folgender Tabelle 6-1 zusammengefasst.

Links unter *Signalpfad* sind darin die Teilstrecken der durch ein konzeptbasiertes System aufgeführt. Die mittlere Spalte gibt die mögliche Technologie zur Realisierung wieder und die rechte Spalte listet die entsprechend zum ASIL erforderlichen SMs oder auch technischen Maßnahmen beim Entwurf eines Systems.

Tabelle 6-1: Übersicht der Kommunikation- und Datenübertragungswege im Konzept

| **Signalpfad** | **Technologie** | **Erforderliche SMs oder -maßnahmen** |
|---|---|---|
| bis e | Mikroelektronik | ASIL A(B), ASIL B(D): Konzept mit AAV<br>ASIL B: separat und integriert einzuplanen |
| E | seriell oder Bussystem | ASIL A(B), ASIL B(D): Konzept mit AAV<br>ASIL B: Ende-zu-Ende-Absicherung |
| e nach z | Mikroelektronik (Teil 1 von MC) | ASIL A(B), ASIL B(D): Konzept mit AAV<br>ASIL B: separat und integriert einzuplanen |
| Z | Bussystem | ASIL B(D), ASIL B: Ende-zu-Ende-Absicherung |

| Signalpfad | Technologie | Erforderliche SMs oder -maßnahmen |
|---|---|---|
| z nach a | Mikroelektronik (Teil 2 von MC) | ASIL A(B), ASIL B(D): Konzept mit AAV<br>ASIL B: separat und integriert einzuplanen |
| A | seriell oder Bussystem | ASIL B(D), ASIL B: Ende-zu-Ende-Absicherung |
| | Parallel | gegeben durch Redundanz der Leitungen |
| | einzelne Signalleitung | ausfallsicherheitsgerichtet<br>ASIL B(D), ASIL B: PWM |
| a nach e' | Mikroelektronik mit Bussystem zwischen den Bausteinen | ASIL A(B), ASIL B(D): Konzept mit AAV |
| e' | seriell oder Bussystem | ASIL A(B), ASIL B(D): Konzept mit AAV |
| Q | seriell oder Bussystem | ASIL B(D): Ende-zu-Ende-Absicherung |
| | Parallel | gegeben durch Redundanz der Leitungen |
| | einzelne Signalleitung | ASIL A(B): ausfallsicherheitsgerichtet<br>ASIL B(D): ausfallsicherheitsgerichtete PWM |

Für Sicherheitsintegritätsstufen unter ASIL B oder ASIL B(D), dekomponiert oder auch nicht, sind im Allgemeinen und normativ gesehen, keine SMs oder zusätzlichen technischen Maßnahmen zum Erreichen ausreichender Sicherheitsintegrität erforderlich.

# 7 EINSATZ ZUR LENKWINKELERFASSUNG

Mit diesem Kapitel wird das im vorangegangenen Kapitel entworfene Konzept zur Lenkwinkelerfassung angewendet und als TSK weiter konkretisiert. Wie in Abschnitt 6.5, „Weitere Vereinfachung durch Integration“ , bereits angekündigt, geht es bei dieser Konzeptanwendung um ein System, bei dem die Vergleichseinrichtung AAV in den zur Sicherheit referenzierten, zweiten Sensorbaustein integriert ist. Der Einsatz des Konzepts setzt auch hier eine serielle, digitale Schnittstelle zwischen den Bausteinen und ein Bussystem zur weiteren Übertragung der sicherheitsgerichteten Daten an verschiedene Empfänger voraus. Diese Konstellation ist für das Beispiel Lenkwinkelsensor praxisorientiert und üblich, weil die Lenkwinkeldaten auf diese Weise in und an allen verschiedenen, über das Fahrzeug verteilten Anwendungen bzw. Einsatzorten genutzt werden können.

## 7.1 ASYMMETRISCHER VERGLEICH BEIM NONIUS-LENKWINKELSENSOR

Das Prinzip des asymmetrisch angesetzten Vergleichs funktioneller Diversität lässt sich sehr gut bei dem in Abschnitt 5.3.1 beschriebenen magnetischen Lenkwinkelsensor anwenden. Dieser besitzt, wie erläutert, zur Ermittlung eines Absolutlenkwinkels über mehrere Lenkradrunden zwei unterschiedlich große Magnetzahnräder, deren Winkelstellungen mit je einem Sensorbaustein vermessen und in einem Rechnersystem nach dem Noniusprinzip zum Absolutwinkel des Lenkrades kombiniert werden. Abbildung 7.1 zeigt links den prinzipiellen Aufbau der Sensorik eines solchen LWS. In der Mitte der Abbildung wird die Funktionsweise nach der Initialisierung und Ermittlung des Absolutlenkwinkels gezeigt, also der Betriebsfall unter neuem Sicherheitskonzept, und rechts ein Foto davon.

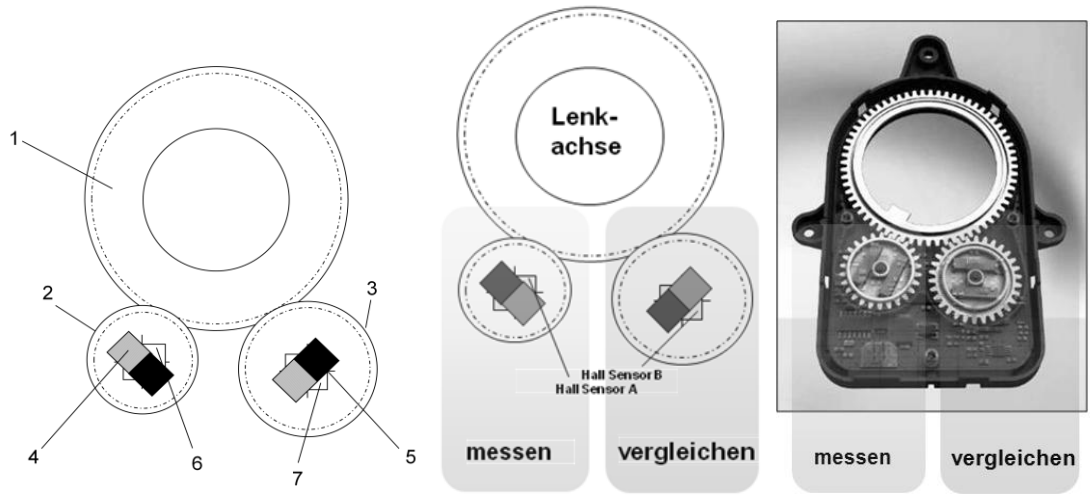



Abbildung 7.1: Prinzip eines magnetischen Lenkwinkelsensors mit Noniusprinzip und AAV

Ein Antriebsrad (1), dessen Drehwinkel bestimmt werden soll, treibt hier zwei Messräder (2, 3) mit unterschiedlichen Radien an. Mit jedem der Messräder (2, 3) ist ein Magnetsystem (4, 5) verbunden, das zusammen mit dem jeweiligen Messrad (2, 3) gegenüber einem ortsfest angeordneten Hall-Sensor (6, 7) verdrehbar ist. Die von den beiden Hall-Sensoren (6, 7) erfassten Drehwinkel sind daher um einen konstanten Faktor verschieden, der sich aus den unterschiedlichen Übersetzungsverhältnissen der beiden Messräder (2, 3) zum Antriebsrad AR (1) ergibt. Während auf der linken Seite noch einmal die bekannte Anordnung dargestellt ist [72], wird in der Mitte und auf der rechten Seite angedeutet, wie der zweite Hall-Sensorbaustein nach Integration einer Vergleichseinrichtung zu Kontrollzwecken herangezogen werden kann. Das erste Magnetrad (2) bleibt Messrad MR, das zweite Magnetrad (3) wird durch Konzeptanwendung zum Kontrollrad KR.

Das LWS-Modul besitzt somit zwei Winkelerfassungssysteme, die sich durch eine lineare Funktion voneinander unterscheiden und somit funktionell diversitär arbeiten können.

Während initial zur Erfassung des Absolutwinkels an Antriebsrad 1 noch beide Messsysteme in gleicher Weise zur Kombination mittels Noniusprinzip benötigt werden, reicht im laufenden Betrieb, wenn es lediglich um Winkeländerungen geht, eines der Messsysteme aus. Das jeweils andere Messsystem steht dann funktionell diversitär zu Absicherungszwecken zur Verfügung. Genau für diese Situation kann also das soweit konzipierte Rechnersystem mit einer asymmetrisch angeordneten Vergleichseinrichtung (AAV) vorteilhaft zur Anwendung kommen. Zur initialen Ermittlung des Absolutwinkels steht dagegen keine geeignete Redundanz zur Erhöhung der Sicherheitsintegrität zur Verfügung, d.h. es wird ausschließlich die Stufe der Sicherheitsintegrität erreicht, die durch Sicherheitsmaßnahmen und eingebaute -mechanismen ohne Sensordiversität möglich ist. Erfahrungsgemäß kann für entsprechende Absolutwinkelausgaben aber trotzdem durchaus ASIL B erreicht werden.

Eine weitere Einschränkung bei der Anwendung des Konzepts zur magnetbasierten Lenkwinkelerfassung mit Noniusprinzip ist die Zyklizität der Messwerte an MR und KR. Hierdurch ist f2 keine Funktion mehr, die nur von a abhängt. Sie hängt auch vom Zustand ab, der sich aus der momentanen Stellung der Messräder zueinander ergibt, weil bei einem Lenkrad mehrere Umdrehungen möglich sind und dadurch auch jeder gemessene Winkel zwischen 0 und 360 Grad eines etwa 1:3 übersetzten Messrades mehrfach auftaucht. Trotzdem gibt es für jede geänderte Stellung des Messrades und den entsprechenden Messwert an MR im Rahmen von normalen Mess- und Rechenungenauigkeiten nur genau einen dazu passenden Kontrollwertbereich an KR, der für die angestrebte Sicherheitsintegrität des Ausgabewerts a steht und dafür ausreicht.

## 7.2 Sicherheitsarchitektur eines konkreten Lenkwinkelsensors

Kurz zusammengefasst wird das im voran gegangenen Abschnitt beschriebene Konzept noch einmal mit der folgenden Abbildung 7.2, nun jedoch mit einer Datenverarbeitungsrichtung von oben nach unten und auf (Hall-sensorisch) gemessene Winkel bezogen.

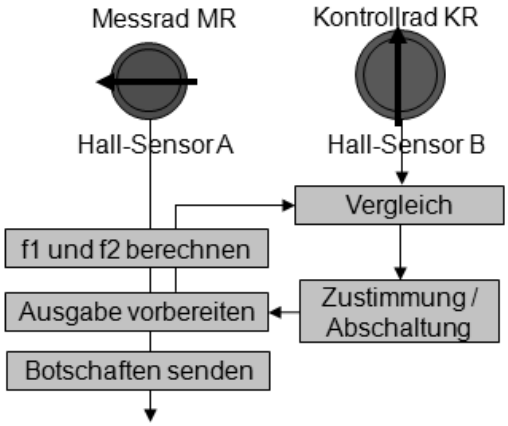



Abbildung 7.2: Winkel am Messrad messen und mit diversitärem Winkel an einem Kontrollrad vergleichen

Dem neuen Konzept entsprechende Sicherheitsarchitekturen für ein Lenkwinkelsensormodul mit Hall-Sensoren könnten wie folgt aussehen (Abbildung 7.3).

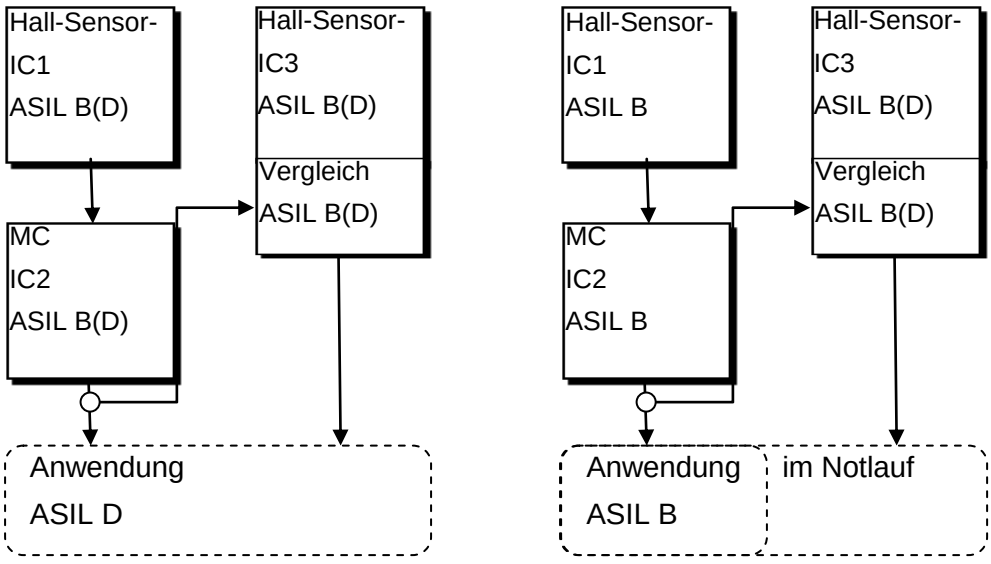



Abbildung 7.3: Mögliche Sicherheitsarchitekturen

Die prinzipiell baugleichen Hall-Sensoren enthalten eine Vergleichseinrichtung, wobei diese im ersten Hall-Sensor-IC1 zunächst nicht benötigt wird. Das Rechnersystem mit

Mikrocontroller MC (IC2) übernimmt die Kontrolle der sensormodulinternen und externen Kommunikation sowie sämtliche Werteanpassungen und Umrechnungen. Alle drei ICs des Sensormoduls werden als sicherheitsbezogene Elemente gemäß ISO 26262 betrachtet. Für Anwendungen mit SZs der Stufe ASIL D muss ihnen jeweils ein ASIL B(D) zugeordnet werden. Für Anwendungen mit SZs bei maximal ASIL B oder auch für den Notlauf von Anwendungen auf ASIL D muss Hall-Sensor-IC1 und das Rechnersystem mit IC2 für die Anforderungen von ASIL B ausgelegt sein. Zur Verbesserung der Integrität für diese Fälle werden natürlich weitere, eingebaute SMs benötigt.

## 7.3 Abläufe im Rechnersystem eines konkreten Lenkwinkelsensors

Das Rechnersystem eines Lenkwinkelsensormoduls unter Anwendung des neuen Konzepts besteht neben seiner Versorgung mit Spannungsregler, eigenem Takt und einem passiven Transceiver für die Buskommunikation im Wesentlichen aus dem Mikrocontroller. Der Mikrocontroller als Kern des Einzel-Rechnersystem im Konzept enthält eine CPU, ROM, RAM, Adress- und Unterbrechungslogik und Schnittstellenperipherie. Die wesentlichen Aufgaben des Mikrocontrollers bestehen zunächst, wie Abbildung 7.4 im linken Teil für den einfachen Fall oder für einen Notlauf auf Stufe ASIL B verdeutlichen soll, aus den beiden Schnittstellen zum Sensor S1 und zum Bussystem und aus einem Winkelanpassungsteil mit zwei Operationen, die hellgrau unterlegt angedeutet sind. Der Ausgabewinkel errechnet sich nämlich wegen des linearen Zusammenhangs zu dem aus S1 gemessenen Winkel über einen vorbestimmten Offset und den Faktor des Übersetzungsverhältnisses von Messrad MR zur Lenksäule.

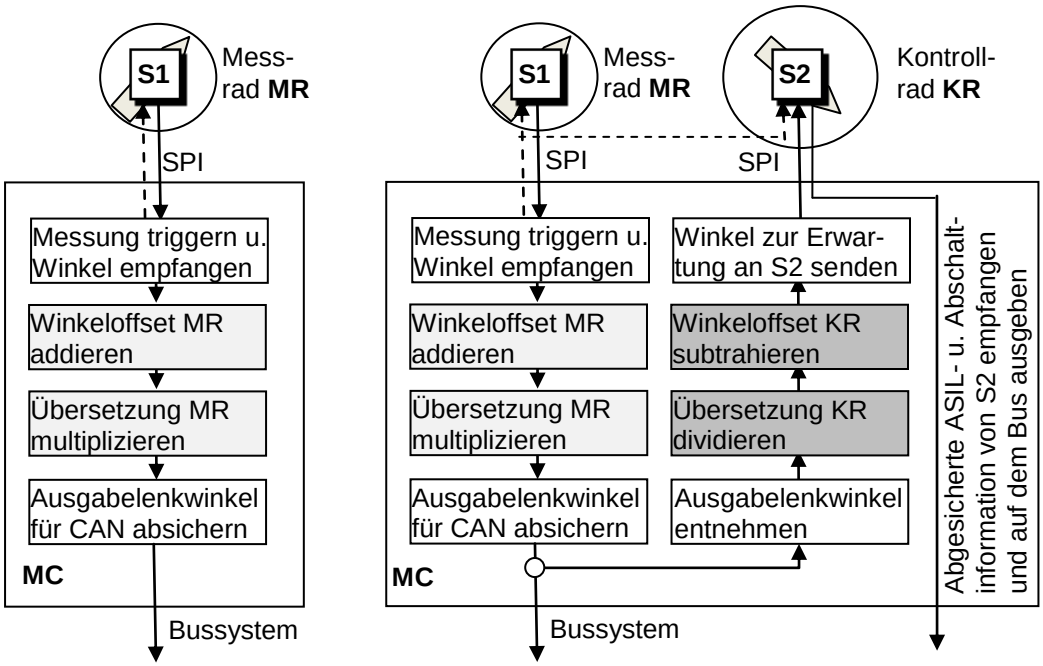



Abbildung 7.4: Aufgaben des Mikrocontrollers im konzeptbasierten magnetischen Lenkradwinkelsensor

Im rechten Teil der Abbildung sind die Aufgaben des Mikrocontrollers für den Fall mit asymmetrisch angeordnetem Vergleich dargestellt. Den beiden aus dem linken Teil bekannten Rechenoperationen stehen die zwei entsprechenden Umkehroperationen, dunkelgrau hinterlegt, gegenüber. Wegen der verschiedenen Radien, Übersetzungsverhältnisse und Drehstellungen der Magneträder sind die behandelten Daten stets systematisch verschieden, weshalb von funktioneller Diversität gesprochen werden kann. Die letzte Aufgabe des Mikrocontrollers MC besteht im Transfer der abgesicherten ASIL- oder Abschaltinformation von S2 unverändert zum Bussystem, wenn diese nicht direkt oder anders an die kritischen, mit ASIL D verknüpften Anwendungen weitergeleitet werden soll.
Übrigens sollte primär das kleinere Magnetrad zur Messung (und nicht zur Kontrolle) verwendet werden, weil wegen der etwas höheren Übersetzung von Lenkachse zu diesem Magnetrad als Messrad auch die Genauigkeit höher ausfällt.

## 7.4 Die Software im Mikrocontroller

Für die Steuerung und Bedienung der digitalen Schnittstellen (SPI, LIN, CAN oder Flexray) und vor allem für die notwendigen Umrechnungen im Mikrocontroller (µC) wird üblicherweise ein SW-System eingesetzt. Dieses ist in seinem Umfang aus Sicherheitsgründen natürlich auf das Nötigste zu beschränken, obwohl das Problem seiner Verifikation gegen sicherheitsrelevante Fehler schon durch das Konzept mit funktioneller Diversität und der AAV gelöst werden wird. Für eine konkrete, sicherheitsgerichtete SW-

Entwicklung sei hier generell auf [73] verwiesen. In diesem Abschnitt sind zunächst die Aufgaben dieses SW-Systems detaillierter zu spezifizieren.

Die in Abbildung 7.4 dargestellten Aufgaben sind noch grob auf das Prinzip reduziert worden. Zur Realisierung in SW soll für diese Aufgaben zunächst eine SW-Architektur bestehend aus drei verschiedenen Schichten entworfen werden. Als Bussystem soll im Folgenden von einem realitätsnahen CAN ausgegangen werden, was für die Anwendung und die Sicherheit des Konzepts unerheblich ist. Jedes andere Bussystem wäre möglich.

Die **erste Schicht** dient der **Abstraktion der Hardware** (en: hardware abstraction layer, HAL). Sie stellt die Treiber und Schnittstellen der SW zur HW des Mikrocontrollers bereit. Mit diesem Teil der SW werden die Register der SPI- und CAN-Peripherie des µCs angesprochen, d.h. Daten und Befehle werden geschrieben oder Daten und Signale werden dort ausgelesen. Die Schnittstellenperipherie des µCs und seine Register sind im Datenblatt oder Handbuch für den Typ des eingeplanten µCs individuell beschrieben. Meistens sind dafür bereits bestimmte SMs in der HW implementiert. Auf diese Weise können einige Übertragungsfehler für LIN, CAN, Flexray und SPI erkannt, in Registern oder durch die Auslösung von Unterbrechungen (Interrupt) angezeigt werden und sollten per SW weiter behandelt werden. Mittlerweile werden besonders zu diesem Zweck standardisierte und fertig qualifizierte SW-Bibliotheken angeboten wie z.B. Autosar im Automobilsektor. Diese sind können sehr umfangreich sein. Aufgrund weitreichender und umfassender Konfigurierbarkeit sind sie sehr komplex und in der Regel nicht vollständig verifiziert. Selbst wenn der asymmetrisch angeordnete Vergleich auch die gefährlichen Fehler, Einwirkungen oder Störungen solcher SW-Teile aufzudecken vermag, sollte nach Möglichkeit auf den Einsatz von nicht leicht selbst verifizierbaren Bibliotheken verzichtet werden. Anders sieht es z.B. mit vom Hersteller des µCs gelieferten Registerdefinitionen oder auch Routinen zum Test der CPU aus.

Eine **mittlere** Schicht übernimmt die zeitliche und Ressourcenkoordination für alle vordergründigen Aufgaben und beinhaltet die Echtzeitunterstützung für eingebettete Systeme. Schon an dieser Stelle sei erwähnt, dass auch diese **Verwaltungsschicht** zur Vermeidung unbeherrschbarer Komplexität auf das Allernötigste beschränkt sein soll. Auf den Einsatz eines kompletten Betriebssystems (en: operating system, OS) oder auch nur eines Echtzeitbetriebssystems (en: real time operating system, RTOS) mit mehreren, nebenläufigen Prozessen (en: multi tasking) und der damit verbundenen Komplexität wird verzichtet. Ideal sind ein einziger, zyklisch aktivierter Prozess für die funktionalen Aufgaben des LWS und möglicherweise ein Hintergrundprozess für verschiedene softwarebasierte Überwachungsaufgaben und Fehlerreaktionen. Diese hier zur Prozessverwaltungsschicht

gehörenden Aufgaben haben mit der eigentlichen Funktion des LWS nichts zu tun und laufen initial, in den Restlaufzeiten der Zyklen der Anwendung und/oder vielleicht beim Anhalten der Anwendung ab. Die Überwachung, im Wesentlichen von ROM, aber auch von RAM, CPU mit ALU[76], Registern und anderen Teilen des µCs, sofern nicht schon per Hardware realisiert, dient im Normalfall, also unter Einbeziehung der Vergleichsinstanz „nur“ zur Erhöhung der Hardwarearchitekturmetrik LFM bei der Beherrschung von MPFs, weil alle PMHF- und SPFM-bezogenen Ausfälle bereits per Vergleichsmechanismus aufgedeckt werden. Nur im Notlauf oder bei Anwendungen ohne Absicherung mit Vergleich dienen die zusätzlichen Überwachungsaufgaben der Erhöhung der PMHF und der SPFM für das µC-Element. Besonders bei Überwachungen, die nicht komplett von der HW des µCs übernommen werden und teils oder ganz in SW realisiert werden, muss abhängig vom vorgesehenen Betriebsmodus (mit oder ohne Vergleichsmechanismus) auf geeignete Überwachungsintervalle geachtet werden. Außerdem müssen auch die SW-Module selbst nach den Anforderungen des entsprechenden ASILs entwickelt werden, je nachdem, welche Art Fehler mit ihnen beherrscht werden sollen. Konkret sollte z.B. ein softwarebasierter Test des ROMs konform zu ASIL A sein, wenn er im Konzept mit Vergleichseinrichtung zur Vermeidung von LFs eingesetzt wird. Für den Einsatz im Notbetrieb einer Anwendung auf ASIL D nach Wegfall der Vergleichseinrichtung und ihrer Ausgaben bzw. für Anwendungen auf ASIL B ganz ohne Vergleichsinstanz, sollte dieser Test zur Vermeidung von SPFs ASIL B erreichen und die dafür spezifizierten FTTIs einhalten.
Gleiches gilt für die Beherrschung von Fehlern im zeitlichen Ablauf im µC, auch wenn der zweite Sensor mit integriertem Vergleich als eine Art Fensterwatchdog angesehen und eingesetzt wird, die sich somit ohne zusätzliche Überwachungssoftware ergibt. Das technische Konzept definiert auch schon die Aufdeckung von Fehlern in den digitalen Signalübertragungsstrecken und ihren HW-Schnittstellen. Dank der vorgesehenen Absicherungen von Datenflüssen durch jeweilige Botschaftszähler und Prüfcodes müssen übertragene Informationen und Signale nicht zusätzlich im Hintergrund überwacht werden.
Die **dritte und letzte Schicht** ergibt sich durch die Module der **Anwendung** (en: application) und realisiert die eigentlichen SW-Funktionen der ECU oder des mechatronischen Moduls. Für einen LWS mit serieller Schnittstelle zu den Sensorbausteinen und einem Bussystem nach außen können diese im Einzelnen mindestens wie folgt definiert werden.

1. Trigger für den Messvorgang in beiden Hall-Sensor-ICs auslösen (CS-Puls)
2. Vordefinierte Zeit abwarten, bis Hall-Sensor-IC1 (S1) bereit zur Ausgabe ist

[76] Arithmetric Logic Unit

3. Messergebnis mit Sensorstatus (aus Eigendiagnose), Zähler und Prüfcode auslesen
4. Prüfcode nachrechnen und validieren
5. Zählerinkrement prüfen (wurde der Zähler seit der letzten Botschaft erhöht?)
6. Sensorstatus (Selbstdiagnosestatus) prüfen und validieren
7. Messergebnis validieren (ist der Wert im gültig definierten Bereich?)
8. Messergebnis als Winkel interpretieren und gemäß linearer Funktion f1 mit Messradkonstanten für Übersetzungsverhältnis aus ROM und Offset aus Kalibrierung zusammen mit aktuellem Rundenmultiplikator (s.u.) zu Absolutwinkel umrechnen
9. Eigendiagnosestatus aus Hintergrundüberwachung prüfen und validieren
10. Absolutwinkel und Botschafts-ID in die CAN-Register eines vorinitialisierten Übertragungsrahmens schreiben
11. Übertragungsrahmen mit inkrementiertem Botschaftszähler versehen
12. Prüfcode (CRC auf Anwendungsebene) über Absolutwinkel und Botschaftszähler im Übertragungsrahmen errechnen und dem Übertragungsrahmen im entsprechenden CAN-Register beifügen (Der Botschaftsrahmen steht ab hier zur Übertragung auf dem CAN bereit)
13. Entnahme des Absolutwinkels aus dem entsprechenden CAN-Register des Übertragungsrahmens
14. Absolutwinkel gemäß linearer Funktion f2 mit Kontrollradkonstanten für Übersetzungsverhältnis aus ROM und Offset aus Kalibrierung umrechnen (Details s.u.)
    (Das Ergebnis ist der erwartete Wert des Winkels am Kontrollrad)
15. Vorausberechneten Wert in vorgegebenem Zeitrahmen per SPI zum Vergleich an Hall-Sensor-IC3 (S2) senden
16. Vordefinierte Zeit abwarten, bis S2 zur Datenausgabe bereit ist
17. Botschaftsrahmen mit abgesichertem Vergleichsergebnis (ASIL-Qualifier) empfangen
18. Botschaftsrahmen von S2 unverändert in die CAN-Register eines weiteren Übertragungsrahmens eintragen und beide CAN-Botschaften absenden.

Die Umrechnungsfunktionen f1 und f2 in der 8. bzw. 14. Funktion oben werden im nächsten Abschnitt 7.4.1 näher beschrieben und später in Abschnitt 7.4.2 beispielhaft implementiert.
Natürlich muss jede Anwendung auch initialisiert werden, d.h. es gibt bei jedem Neustart des LWS-Moduls noch die Aufgabe, Variablen, Daten, Peripherieregister etc. auf definierte Werte bzw. Einstellungen zu setzen.

Die Anforderungen an ein reales SW-System eines Lenkwinkelsensormoduls gehen in der Regel weit über die bisher vorgestellten Schnittstellen- und Umrechenaufgaben hinaus.
Zu nennen sind hier zunächst die folgenden Funktionen.

- **Errechnung** des Winkelgradienten, d.h. der Winkelgeschwindigkeit mit Hilfe einer Winkelhistorie und Bezug zur Messzykluszeit.
- **Überwachung** der physikalisch maximal möglichen Winkeländerung (30°/10 ms)
- **Korrektur** der Integralen Nichtlinearität (INL), z.B. anhand einer nach Kalibrierung gespeicherten Tabelle um maximal ±1,5°

Zur Errechnung des Winkelgradienten werden Winkelmesswerte ausschließlich gelesen und, nach dem Verlassen des sicherheitsgerichteten Signalpfads für Lenkwinkel gespeichert. Anschließend werden aus den abgezweigten Winkeldaten Winkeldifferenzen ermittelt und auf die vergangenen Zwischenzeiten bezogen. Dabei entstehen Gradienten, für die mit diesem Konzeptansatz maximal ASIL B erreicht wird. Die Daten werden über das Bussystem, allerdings unabhängig und neben dem sicherheitsgerichteten Pfad für Lenkwinkel, an die Anwendungen übertragen, die diese Information benötigen. Eine sicherheitsgerichtete Verwendung solcher Informationen würde natürlich die Definition und Verfolgung separater SZs erfordern.
Auch bei der Überwachung der maximal möglichen Winkeländerung handelt es sich um eine Zusatzfunktion, die ausschließlich lesend auf die Daten des sicherheitsgerichteten Pfads zugreift. Fehler in dieser (Schutz-)Funktion werden bestenfalls zur Abschaltung der sicherheitsgerichteten Funktion des LWS führen und damit als sicher angesehen werden.
Etwas anders sieht es bei der Korrektur der Absolutwinkeldaten aus. Hier wird der errechnete Absolutwinkel im sicherheitsgerichteten Pfad nachträglich verändert, also schreibend auf ihn zugegriffen. Die Korrekturwerte sollten allerdings auf vielleicht unkritische ±1,5° (bezogen auf das Lenkrad) begrenzt werden. Dies wird durch eine fest vorgegebene Tabelle erreicht, die entweder allgemein für die Mechanik ermittelt oder, noch genauer, individuell für jeden LWS kalibriert und für den späteren Betrieb im Speicher hinterlegt wird.
Alle diese Aufgaben können innerhalb desselben Prozesses erledigt werden. Ein nebenläufiger, die Komplexität des SW-Systems erweiternder Prozess ist dafür nicht notwendig.
Die verschiedenen, angesprochenen Schutz- und Überwachungsmechanismen (SMs) benötigen zur Beibehaltung eines sicheren Zustands auch entsprechende Fehlerbehandlungen. Diese bestehen wiederum aus kleinen Funktionen in allen drei vorgestellten Architekturschichten und führen je nach Ergebnis einer Sicherheitsanalyse zum Neustart einzelner

Hall-Sensor-ICs oder des gesamten Rechnersystems oder zum Stopp des Botschaftsversands von Lenkwinkel- oder Integritätsdaten zu den Anwendungen per CAN.
Weitere Anforderungen an einen praxisorientierten LWS reichen von Möglichkeiten zur mehr oder minder umfangreichen Diagnose über SW-Download per CAN bis zu Konfigurations- und Kalibriermodi, die vom SW-System unterstützt werden sollen. Wenn sich solche SW-Teile nicht von vorne herein im selben SW-System vermeiden lassen, muss zumindest ihr Einfluss auf die sicherheitsgerichteten Pfade unterbunden werden, beispielsweise durch eine Partitionierung im µC, die von der HW des µCs unterstützt wird.
Andere Zusatzfunktionen oder -funktionalitäten für ein Rechnersystem im LWS könnten bereits im Sensormodul realisierte Anwendungen wie Müdigkeitserkennung oder eine Blinkerrückstellung sein. Auch Funktionen, die nichts mit dem Lenkwinkel zu tun haben, werden bei der Entwicklung eines Lenksäulenmoduls wie dem LWS erwogen, um einmal vorhandene Prozessorressourcen mitzuverwenden. Dies böte sich z.B. bei Sensorik für den Blinker-, Wischer-, Licht-, Automatikschalthebel oder kombinierte Hebel am Lenkrad an. Vielleicht wird in der Praxis aber auch eine Gateway-Funktion erwogen, um Informationen zwischen Lenkrad und Fahrzeugsystem über verschiedene Schnittstellen auszutauschen (z.B. für Multifunktionstaster, Horn, etc.).
Zu Gunsten von Funktionssicherheit und deshalb zur strengen Vermeidung von Komplexität wird man für Lenkwinkelsensoren, die für kritischste Anwendungen zum Einsatz kommen sollen, auf alle zusätzlichen und softwarebasierten Funktionen nach allen Möglichkeiten verzichten müssen. Ideal für diese Anwendung ist ein LWS, der nur das Notwendige für eine ausreichende Genauigkeit und das SZ mit dem höchsten ASIL beinhaltet und leistet. Für die weniger sicherheitsgerichteten Anwendungen ist stattdessen ein separater LWS einzuplanen, der alle zusätzlich benötigten Funktionen besitzt und die übrigen Anforderungen erfüllt.

### 7.4.1 UMRECHNUNGSFUNKTIONEN

Die linearen Funktionen zur Umrechnung eines Messwertes zum Winkelwert und des Winkelwerts zum Kontrollwert für den zweiten Sensor sind:

**Winkelwert = f1(Messwert)** und **Kontrollwert = f2(Winkelwert)**.

Funktion f1 muss einen vorab bestimmten Offset addieren und einen Faktor multiplizieren. Der Offset besteht aus der Winkeldifferenz zwischen Lenkrad LR und Messrad MR und aus einem Korrekturwert zum Abgleich des Nullpunkts, der bei einer Kalibrierung während der Herstellung ermittelt wurde. Der Faktor der Funktion setzt sich zusammen

aus der bekannten Übersetzung zwischen Lenkrad AR und Messrad MR und einem Faktor zur Normierung des Ausgabewertes als Winkelwert auf dem Bussystem CAN zum Gebrauch in der Anwendung.
Die entgegen gerichtete Funktion f2 muss die entsprechend auf das Kontrollrad KR bezogenen Konstanten verwenden.
Unter Annahme konkreter Magneträder mit anwendungserprobten Zähnezahlen (LR 74, MR 26, KR 30) und der Nullstellung aller Magneträder bei einem Absolutwinkel von ±0 Grad (Geradeausfahrt) sehen die Linearfunktionen wie folgt aus.

$$f1(x) = \frac{26}{74} \cdot \frac{3600}{2^{14}} \cdot x = 0{,}0772 \cdot x \text{ und } f2(x) = \frac{74}{30} \cdot \frac{2^{14}}{3600} \cdot x = 11{,}226 \cdot x$$

Die Konstante 3600 darin ist einer Normierung der Winkel auf 10tel Grad auf dem CAN geschuldet und der Wert $2^{14}$ rührt her aus der Normierung von $2^{14}$ Inkrementen eines anwendungserprobten Hall-Sensor-ICs für den Bereich von 360°.
Für die Ausgabe eines Winkelwerts über mehrere Lenkradrunden müssen in f1 die Übergänge in weitere Runden MRR des Messrades in positiver oder negativer Richtung mitgezählt und jeweils als Vielfaches der Inkremente für 360° addiert bzw. subtrahiert werden. Die Umrechnungsfunktion f1 für den Absolutlenkwinkel (Winkelwert) sieht dann folgendermaßen aus.

$$f(x) = \frac{26}{74} \cdot \frac{3600}{2^{14}} \cdot (x + 2^{14} \cdot MRR) = 0{,}0772 \cdot x + 1264{,}865 \cdot MRR$$

In der entgegen gerichteten Funktion f2 muss das Ergebnis am Ende noch durch das Vielfache von $2^{14}$ der weitergezählten Kontrollradrunde KRR dividiert werden (der Einfachheit halber Modulo $2^{14}$), bis der Kontrollwert im Bereich von ±180° liegt (Intervall [0°, ... , 360°]) und als Wert < $2^{14}$ zum Vergleich in Hall-Sensor-IC3 (S2) übrig bleibt. Ist der Betrag am Ende der Berechnung größer, so deutet dies auf einen Fehler hin, der bezüglich sicherem Zustand behandelt werden muss.
Je nach Implementierung der Funktionen f1 und f2 sind natürlich Rechenungenauigkeiten zu erwarten, die sich, zumindest wegen der von f1, bei der Gesamtgenauigkeit des ausgegebenen Absolutwinkels geringfügig bemerkbar machen.
Bei den beiden nun vorhandenen Funktionen f1 und f2 muss nur noch folgender Aspekt berücksichtigt werden. Es ist nicht davon auszugehen, dass bei jedem Neustart des LWS das Lenkrad zur Geradeausfahrt ausgerichtet ist. Wahrscheinlicher ist dagegen eine Lenk-

radstellung, die eine ganz bestimmte Konstellation von Winkelstellungen für Mess- und Kontrollrad verursacht, die auf zwei dadurch festgelegte, unterschiedliche Rundenzahlen (MMR bzw. KRR) für Mess- und Kontrollrad schließen lässt. Beim Start des LWS muss es also initial noch eine Routine geben, die den Messwert aus Hall-Sensor-IC1 (S1) in Bezug zu dem an dieser Stelle aus S2 gelesenen Messwert stellt und nach dem Noniusprinzip aus dem Verhältnis beider Winkel die momentan richtige Messradrunde MRR und Kontrollradrunde KRR ermittelt[77]. Diese Daten können z.B. aus einer fest einkodierten Winkelbereichstabelle wie in Tabelle 7-1 angedeutet entnommen werden. Die Tabelle mit 30° Differenz pro Messradumdrehung zwischen den beiden Magneträdern geht dabei von einem Zähneverhältnis von 36 zu 39 zwischen Messrad zu Kontrollrad aus.

Tabelle 7-1: Auszug einer Winkelbereichstabelle zur Anwendung des Noniusprinzips

| α aus S1 / β aus S2 | 0°..30° | 30°..60° | 60°..90° | 90°..120° | 120°..150° | 150°..180° |
|---|---|---|---|---|---|---|
| 0°..25° | MRR: 0<br>KRR: 0 | MRR: 1<br>KRR: 1 | MRR: 2<br>KRR: 2 | MRR: 3<br>KRR: 3 | MRR: 4<br>KRR: 4 | MRR: 5<br>KRR: 5 |
| 25°..50° | MRR: 11<br>KRR: 10 | MRR: 0<br>KRR: 0 | MRR: 1<br>KRR: 1 | MRR: 2<br>KRR: 2 | MRR: 3<br>KRR: 3 | MRR: 4<br>KRR: 4 |
| 50°..75° | MRR: 10<br>KRR: 9 | MRR: 11<br>KRR: 10 | MRR: 0<br>KRR: 0 | MRR: 1<br>KRR: 1 | MRR: 2<br>KRR: 2 | MRR: 3<br>KRR: 3 |
| 75°..100° | MRR: 9<br>KRR: 8 | MRR: 10<br>KRR: 9 | MRR: 11<br>KRR: 10 | MRR: 0<br>KRR: 0 | MRR: 1<br>KRR: 1 | MRR: 2<br>KRR: 2 |
| 100°..125° | MRR: 8<br>KRR: 7 | MRR: 9<br>KRR: 8 | MRR: 10<br>KRR: 9 | MRR: 11<br>KRR: 10 | MRR: 0<br>KRR: 0 | MRR: 1<br>KRR: 1 |
| 125°..150° | MRR: 7<br>KRR: 6 | MRR: 8<br>KRR: 7 | MRR: 9<br>KRR: 8 | MRR: 10<br>KRR: 9 | MRR: 11<br>KRR: 10 | MRR: 0<br>KRR: 0 |

Durch geschickte Wahl von Übersetzungsverhältnissen können die Rechnungen bei der Implementierung vereinfacht und rechengenauer durchgeführt werden. Zum Beispiel bei einem gewählten Zähneverhältnis von 225 am Antriebsrad der Lenkachse zu 64 am Messrad muss man den um Offset und Runden korrigierten Messwert nur durch 16 teilen (4 Bitpositionen nach rechts schieben), um den Absolutwinkelwert direkt in Zehntelgrad ablesen zu können. Im Kontrollweg für f2 muss der Absolutwinkelwert mit 1024 multipliziert (10 Bitpositionen nach links schieben) und alsdann durch 69 geteilt werden, um ihn bei einem Zähneverhältnis von 225 zu 69 am Kontrollrad vergleichen zu können. Der Messbereich für die Lenkspindel bzw. das Lenkrad würde damit ausreichend knapp 4 Runden umfassen (69/(69-64) · 64/225).

[77] Wie weiter oben erläutert, ist diese Absolutwertbestimmung zur Laufzeit durch keine (weitere) Redundanz überprüfbar und erreicht für ihre Ergebnisse maximal die Sicherheitsintegritätsstufe ASIL B.

### 7.4.2 IMPLEMENTIERUNG DER SOFTWARE IM MIKROCONTROLLER

Die Aufgaben der SW im Mikrocontroller nach der Initialisierung werden regelmäßig durch ein zyklisch generiertes Timer-Event gestartet, beispielsweise jede Millisekunde. Vorgesehen ist eine serielle Übertragung von Botschaften zwischen den einzelnen Bausteinen, sowohl was die Winkelinformationen als auch was das Vergleichsergebnis betrifft. Die wesentlichen Teile sollen durch den wie folgt dargelegten Quelltext mit der Syntax und dem limitierten Sprachumfang der Sprache C90 [74] verdeutlicht werden.

```
// Konstanten definieren:
#define K0 0                // Konstante für Null
#define K26 26              // Konstante für Zähnezahl Messrad MR
#define K30 30              // Konstante für Zähnezahl Kontrollrad KR
#define K74 74              // Konstante für Zähnezahl Antriebsrad AR
#define Maske_0x3FF 0x3FF   // Konstante Bitmaske für 2^10 - 1
#define K2P13 8192          // Konstante für 2^13
#define K2P14 16384         // Konstante für 2^14
#define K3600 3600          // Konstante für 3600 Zehntelgrad

// Typen definieren:
typedef struct {            // Telegrammtyp definieren
      unsigned short id;
      unsigned short winkel; // alternativ hier das Vergleichsergebnis
      unsigned short status;
      unsigned char bz;
      unsigned char crc;
} Telegramm;

typedef struct {            // Botschaftstyp definieren
      short id;
      short absWinkel;
      unsigned short status;
      unsigned char bz;
      unsigned char crc;
} Botschaft;

// Globale Variablen definieren:
Telegramm tVonS1, tAnS2, tQ; //Speicher für SPI-Botschaften
Botschaft bY; // Speicher für CAN-Botschaft

// Funktionen deklarieren:

// Offset zum Messrad MR aus dem Konfigurationsspeicher holen
int HinterlegterOffsetMR(void);

// Offset zum Kontrollrad KR aus dem Konfigurationsspeicher holen
int HinterlegterOffsetKR(void);

// Hilfsfunktionen zum Verwalten (Setzen/Lesen) der Messradrunde
// (wird unter Noniusprinzip  Initialisierung gesetzt)
void SetRundeMR(int r); // Setze die aktuelle Runde des Messrades MR
int GetRundeMR(void); // Hole die aktuelle Runde des Messrades MR
```

```
// Zyklisch aufgerufene Hauptfunktion
void messeZyklisch(void);

// In beiden Sensoren einen synchronen Messvorgang auslösen
void triggere_Sensoren_1_und_2(void);

// Messwerttelegramm aus S1 auslesen
void lies_Sensor_1(Telegramm *pT);

// Id, CRC8 und Botschaftszähler überprüfen
void pruefe_Integritaet_Telegramm(Telegramm *pT);

// Integrität des Sensors sicherstellen; Sensorstatus prüfen
void pruefe_Integritaet_Sensor1(Telegramm *pT);

// Messwert auf Absolutwert umrechnen
void rechne_um_auf_Absolutwinkel(Telegramm *pT, Botschaft *pB);

// Botschaft für CAN mit Id, CRC und Botschaftszähler erstellen
void erstelle_CAN_Botschaft(Botschaft *pB);

// Absolutwert aus abgesicherter CAN-Botschaft aufgreifen
// und auf Vergleichswert umrechnen
void rechne_um_auf_erwarteten_Wert(Botschaft *pB, Telegramm *pT);

// Vergleichsbotschaft erstellen
void erstelle_Vergleichsbotschaft(Telegramm *pT); // CRC

// Vergleichsbotschaft an S2 unter Kontrollrad senden
void sende_SPI_Sensor2(Telegramm *pT);

// Warten, bis S2 verglichen und reagiert hat (Timeout)
// und Vergleichsergebnis auslesen
void erwarte_Qualifier_TO_100Mikrosekunden(Telegramm *pT);

//CAN-Botschaft entsprechend der Id in Botschaft absenden
void sende_CAN_Botschaft(Botschaft *pB);

// Funktionen definieren:

// Funktion f1(e)
void rechne_um_auf_Absolutwinkel(Telegramm *pT, Botschaft *pB)
{
      int Messwert = K0;

      // 2^14 Inkremente entsp. 360° => 1 Inkr. entspricht 0,021973°

      // Messwert_aus_Botschaft_extrahieren:
      Messwert = (int)pT->winkel & Maske_0x3FF // Maske für 14 LSBs

      // Messwert mit Vorzeichen behaften (max. +- (2^13 - 1)) und
      // Offset für Messrad MR aus der Initialisierung addieren
      if (Messwert >= K2P13) // >= 180° ?
      {
```

```
            Messwert = - (K2P14 - Messwert); // max. -180°

            // Offset für Messrad MR aus der Initialisierung addieren
            Messwert = Messwert + HinterlegterOffsetMR();
            if (K0 <= Messwert) // nächste Runde dieses Messrades?
            {
                  SetRundeMR(GetRundeMR() + 1); // Ja!
            }
      }
      else
      {
            // Vorzeichen bleibt positiv
            // Offset für Messrad MR aus der Initialisierung addieren
            Messwert = Messwert + HinterlegterOffsetMR();
            if (K0 > Messwert) // vorige Runde dieses Messrades?
            {
                  SetRundeMR(GetRundeMR() - 1); // Ja!
            }
      }

      // Messwert auf Absolutw. umrechnen (+- die Runden des Messrades)
      Messwert = Messwert + (GetRundeMR() * K2P14); // MR-Runden*360°

      // Messwert_auf_Antriebsrad_umrechnen:
      Messwert = Messwert * K26;    // Zähneverhältnis 26 / 74
      Messwert = Messwert / K74;    // entspricht 1/Mw = 2,846

      // Messwert_auf_CAN_Größe_normieren (Zehntel-Grad, 0,1°/Inkr.)
      Messwert = Messwert * K3600; // mit 3600 multiplizieren
      Messwert = Messwert / K2P14; // durch 2^14 teilen

      pB->winkel = (short)Messwert;
}

// Funktion f2(a)
void rechne_um_auf_erwarteten_Wert(Botschaft *pB, Telegramm *pT)
{
      int Messwert = K0;

      // Messwert_von_CAN_auf_Messgröße_normieren
      // (Zehntel-Grad -> 0,021973°/Inkr.):
      Messwert = K2P14 * (int)pB->winkel; // mit 2^14 multiplizieren
      Messwert = Messwert / K3600; // durch 3600 teilen

      // Messwert_von_Antriebsrad_auf_Kontrollrad_umrechnen
      Messwert = Messwert * K74;    // Zähneverhältnis 74 / 30
      Messwert = Messwert / K30;    // entspricht m = 2,466

      // Messwert_von_Absolutgröße_auf_Messrad_umrechnen
      Messwert = Messwert % K2P14; // S2-Runden*360° mit Modulo-Befehl

      // Offset für Kontrollrad KR aus der Initialisierung subtrahieren
      Messwert = Messwert - HinterlegterOffsetKR();

      // Messwert von Vorzeichen befreien
```

```
      if (Messwert < K0) // < 0° ?
      {
            // Es muss ein Wert für maximal 359,9° entstehen
            Messwert = Messwert + K2P14;
      }
      else
      {
            // Vorzeichen bleibt positiv
      }

      // der so gewonnene Messwert muss nun mit dem Kontrollwert
      // in S2 mit geringer Toleranz übereinstimmen.
      pT->winkel = (unsigned short)Messwert;
}

// folgende Funktion wird regelmäßig als Task per Scheduler aufgerufen
void messeZyklisch(void) // z.B. alle 1000 µs
{
      triggere_Sensoren_1_und_2();

      //Daten von S1 empfangen, wg. Genauigkeit am kleineren Messrad
      lies_Sensor_1(&tVonS1); // 64-Bit breite Botschaft als SPI-Master

      // Id, CRC8 und Botschaftszähler überprüfen
      pruefe_Integritaet_Telegramm(&tVonS1);

      //Integrität des Sensors sicherstellen
      pruefe_Integritaet_Sensor1(&tVonS1);

      //Messwert auf Absolutwert umrechnen
      rechne_um_auf_Absolutwinkel(&tVonS1);

      //Botschaft für Bussystem erstellen
      erstelle_CAN_Botschaft(&tVonS1, &bY); // Id, CRC und BZ

      //Absolutwert auf Vergleichswert umrechnen
      rechne_um_auf_erwarteten_Wert(&bY, &tAnS2);

      //Vergleichsbotschaft an S2 erstellen
      erstelle_Vergleichsbotschaft(&tAnS2); // CRC

      //Vergleichsbotschaft an S2 unter Kontrollrad senden
      sende_SPI_Sensor2(&tS2);

      //Warten und Vergleichsergebnis von S2 mit TimeOut empfangen
      erwarte_Qualifier_TO_100Mikrosekunden(&tQ);

      //CAN-Botschaften absenden
      sende_CAN_Botschaft(&bY);
      sende_CAN_Botschaft((Botschaft*)&tQ);
}
```

## 7.5 DIE ASYMMETRISCH ANGEORDNETE VERGLEICHSEINRICHTUNG

Kern des neuen Konzepts ist der asymmetrisch angeordnete Vergleich der vorhandenen funktionellen Diversität. Die entsprechende Einrichtung dafür (AAV) sollte möglichst trivial ausfallen, um erstens sie umso einfacher für hohe systematische Sicherheitsintegrität verifizieren zu können und zweitens auch mit geringem Aufwand die normativ geforderten Diagnosedeckungsgrade und Zielwerte für die Sicherheitsmetriken PMHF, SPFM und LFM zum Nachweis ausreichender HW-Integrität zu erreichen.
Zur Realisierung dieser im Sensorbaustein integrierten Vergleichseinrichtung stehen grundsätzlich Analog- wie auch Digitaltechnik zur Verfügung, da ein Hall-Sensor-IC wie der in Abschnitt 5.2.3 beschriebene Baustein MLX90363 auf seinem Silizium-Die beide Techniken miteinander vereint. Ein mögliches Blockschaltbild für einen solchen Baustein mit analoger Vergleichseinrichtung ist in Abbildung 7.5 wiedergegeben.

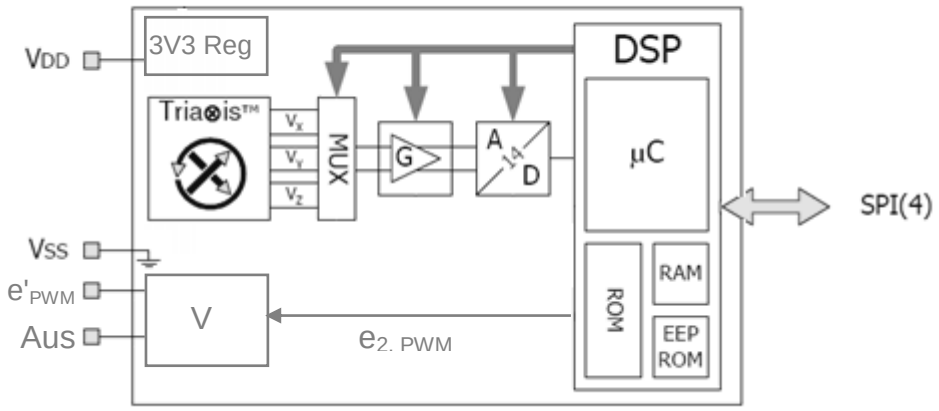



Abbildung 7.5: Blockschaltbild S2 mit rein hardwarebasierter Vergleichseinrichtung

Ein Vergleich im Analogteil des Sensor-Chips zieht zwei den zu vergleichenden Winkelwerten entsprechende, elektrische Spannungen heran, die durch PWM-Ausgaben der Digitalteile in MC und in S2 erzeugt werden. Konkret sieht der Vergleich der beiden Spannungen dann wie folgt aus, wenn man beispielsweise 3,6V für 360 Winkelgrad zugrunde legt und eine Fehleraufdeckung von 99% erreichen möchte. Ein in Analogtechnik integrierter Spannungskomparator vergleicht die Spannungen auf ± 18mV genau. Die beiden Spannungen müssen also innerhalb eines Toleranzbereichs von 36mV hin zusammenpassen, um die Abschaltreaktion am Ausgang „Aus“ einer solchen Vergleichseinrichtung zu vermeiden. Dieser Bereich entspricht einem Bereich von 3,6° am Kontrollrad, der angesichts einer Messgenauigkeit des in Erwägung gezogenen Magnetsensors von 1° recht weit gefasst ist und mit dem mechanische Genauigkeitsverluste durch Hysterese, Nichtlinearitäten

etc. ausreichend berücksichtigt sein sollten. 3,6° am Kontrollrad entsprechen bei einer Übersetzung von beispielsweise 1:3 vom Antrieb her dort nur 1,2°.
Da es sich wegen der Drehrunden von Mess- und Kontrollrad um zyklisch wiederkehrende Winkelwerte im Bereich 0° bis 360° handelt, muss beim Vergleich die Möglichkeit beachtet werden, dass der eine Winkelwert gerade eine neue Runde erreicht hat, während der zweite Winkelwert die 360° noch knapp nicht erreicht hat und gerade vor dem Rundensprung steht.
Für ein die Übereinstimmung der Werte anzeigendes Ergebnis des Vergleichs muss demnach auch definiert sein, dass bis maximal zum Toleranzbereich (im Beispiel bis 36 mV) kleine Größen auch mit Größen zusammenpassen, die im Beispiel mindestens 3600 mV + kleine Größe – 36 mV groß sind. Eine Lösung für das Problem besteht darin, eine Abweichung der beiden Winkel von mehr als Gesamtbereich minus Toleranzbereich ebenfalls als passend zueinander werten zu lassen.
Auch bei der digitalen Realisierung einer Vergleichseinrichtung, von der in den vorangegangenen Abschnitten ausgegangen wurde, muss natürlich die Periodizität der Winkelwerte beachtet werden. Die hierzu notwendige Fallunterscheidung lässt sich sicherlich weniger aufwändig als in Analogtechnik umsetzen.
Die Realisierung der Vergleichseinrichtung mit konfigurierbarem Toleranzbereich in Digitaltechnik wäre gegenüber der rein hardwarebasierten Lösung nur wenig komplexer. Dazu bietet sich die Firmware eines Sensors an, wie sie der vorgestellte Hall-Sensor-Chip MLX90363 für die trigonometrischen Funktionen und Analogteildiagnosen ohnehin besitzt. Die beiden Eingangswerte für Kontrollmesswert in S2 und Vergleichswert aus MC werden dazu zunächst für jeden Vergleich digital und direkt in zwei antivalent initialisierte Variablen übernommen. Der Vergleich selbst kann dann mit folgendem Pseudocode spezifiziert werden.

```
kw = Kontrollmesswert // aus S2
vw = Vergleichswert // aus MC
if (kw > MaxWert) oder (vw > MaxWert) // Konstante MaxWert ist 2^14 – 1 = 16383
       error „Bereichsfehler“
if (kw > vw)
       diff = kw – vw
else
       diff = vw – kw
if (diff > Toleranzbereich) // Toleranzbereich ist hier konst. 2^14 / 100 = 164
       if (diff < MaxWert – Toleranzbereich) // zweiter Fall: Rundenversatz
              error „keine Übereinstimmung -> Fehlerreaktion zur Abschaltung“
return // Übereinstimmung
```

Die Implementierung der so spezifizierten Vergleichseinrichtung ist trivial und durch die einfachsten Sprachelemente von PEARL oder auch C realisierbar. Sofern für entsprechende Sicherheit erprobte oder qualifizierte Werkzeuge zur Übersetzung der Quelltexte zur Verfügung stehen, kann die fertige Lösung der in S2 integrierten Software/Firmware hinzugefügt werden. Ergänzt werden müssen lediglich entsprechende Fehlerreaktionen in HW und/oder SW (siehe nächster Abschnitt für Details). Für den softwarebasierten Abschaltpfad ist konzeptionell vorgesehen, das Vergleichsresultat vor der seriellen Übertragung durch vorverifizierte Ende-zu-Ende-Absicherungen (Identifikation, Botschaftszähler, CRC) zu erweitern.

## 7.6 Das Erreichen und Halten sicherer Zustände

Abgesehen von den Fehlerreaktionen und Abschaltpfaden der oben schon erwähnten SMs im SW-System des LWS muss es natürlich auch für die externe Vergleichseinrichtung in Hall-Sensor-IC3 (S2) geeignete Möglichkeiten zum Beibehalten eines sicheren Zustands oder zum Übergang in einen anderen sicheren Zustand geben. Bei einer Dekomposition zwischen Funktions- und Schutzpfad zu jeweils ASIL B(D) muss sich der gesamte Abschaltpfad auf dieser Sicherheitsintegritätsstufe befinden. Möglichkeiten und Bedingungen hierzu sollen nun Thema dieses Abschnitts und seiner Unterabschnitte sein.

Die asymmetrisch angeordnete Sicherheitsvergleichseinrichtung in S2 vergleicht zwei digital vorliegende Winkelinformationen mit 14 Bit Breite: den vom Mikrocontroller vorausberechneten Wert zur Erwartung in Hall-Sensor-IC3 und der in ihm selbst gemessenen Kontrollwert. Beide Werte werden zunächst in einem definierten Zeitfenster erwartet und überwacht. Nicht verfügbare Vergleichswerte werden als Fehler interpretiert und lösen das Abschaltsignal aus. Als Nächstes werden die beiden Werte miteinander in einem vorkonfigurierten Toleranzfenster verglichen, das eine konfigurierbare Begrenzung von maximal ±12° von 360° hat und je nach Genauigkeit der Mechanik und der Hall-Sensor-ICs abgestimmt und eingestellt werden muss. Beim Vergleich in Digitaltechnik müssen genügend signifikante Bits der beiden Vergleichswerte auf Übereinstimmung geprüft werden können, um die Integrität der Winkelmessungen, der Hall-Sensor-ICs und des µCs sicher stellen zu können.

Stimmen die Werte nun überein, so wird der in jedem Messzyklus als Default eingerichtete Abschaltwert (aktiv) aufgehalten bzw. mit einem für die erreichte Integrität stehenden Wert überschrieben.

S2 (samt AAV) als Sicherheitselement muss für ASIL B(D) imstande sein, eigene Fehler mit Potential zur Verletzung des SZs im Rahmen der Fehlertoleranzzeitintervalle zu mindestens 90% zu beherrschen (s. z.B. ISO 26262-5, Klausel 9.4.2.5). Dies kann bereits durch den für jeden zyklisch gemessenen und ausgegebenen Absolutwinkel durchgeführten Vergleich erreicht werden. Weiter fordert ein ASIL B(D) für S2, dass MPFs zu mindestens 60% gegen ihr latent gefährliches Auftreten zu beherrschen sind, wenn auch nicht unter denselben zeitlichen Vorgaben. Diese Fehler, z.B. an integrierten SMs wie durch den Vergleich selbst oder wenn an S2 Überspannung anliegt, können nur durch weitere SMs diagnostiziert werden. Deren Fehlerreaktionssignale können zwecks Beherrschung entweder in das Abschaltsignal der Vergleichseinrichtung mit einbezogen werden, oder als separates Abschaltsignal ausgegeben werden. Das in Abschnitt 5.2.3 vorgestellte Hall-Sensor-IC zum Beispiel hat, selbst bis 18V spannungsfest, eine eingebaute Spannungsüberwachung, mit der eine am Rechnersystem anliegende und gefährliche Überspannung erkannt werden kann. Die Erkennung wird direkt als Abschaltsignal per HW und konfiguriert als Abschaltinformation oder als Diagnosestatus im Rahmen des firmwarebasierten SPI-Protokolls ausgegeben.

Die Abschaltinformationen der Vergleichseinrichtung in S2 des Konzepts können grundsätzlich ebenfalls per HW-Leitung oder per softwarebasiertem, seriellem Protokoll (Botschaft) ausgegeben werden. Die folgenden beiden Abschnitte werden diese beiden Abschaltarten, die natürlich auch kombiniert werden dürfen, jeweils beleuchten.

Weiter oben wurde für das Sicherheitskonzept bereits festgehalten, dass es darauf basiert, dass jedes hardware- oder softwarebasierte Signal, das das betrachtete Modul nicht oder nicht rechtzeitig verlässt, (ausfallsicherheitsgerichtet) als sicher gilt und zu einem sicheren Zustand führt. Dies soll nun insbesondere für das Vergleichsergebnis und die davon ausgehenden Abschaltdaten in jeder ausgegebenen Form und für jeden Wert gelten. Auch hier soll in den beiden folgenden Abschnitten entsprechend unterschieden werden.

### 7.6.1 Abschaltung per Hardware

Die einfachste (und damit sicherste) Art der Abschaltung ist die per Hardwaresignal. Da der sichere Zustand in der Regel mit Inaktivität verknüpft ist, sollte die vom Hall-Sensor-IC auf einer elektrischen Leitung ausgegebene Abschaltinformation im Idealfall aus der Abschaltung einer im Normalfall aktivierenden Spannung bestehen. Fehler an dieser Leitung selbst sind aller Wahrscheinlichkeit nach Unterbrechungen, die in dieser ausfallsicherheitsgerichteten Logik bereits einen sicheren Zustand herstellt. Eine Leitung mit dieser Logik kann daher als eigensicher betrachtet werden. Ziel jeder Abschaltinformation ist eine Unterbrechung oder zumindest eine für den Notlauf geplante Einschränkung der

sicherheitsgerichteten Funktionalität. Die angesprochene Hardwareleitung mit im Fehlerfall deaktivierender Wirkung könnte nun z.B. LWS-intern zur Abschaltung des Mikrocontrollers, des CAN-Transceivers oder beispielsweise der TX-Sendeleitung genutzt werden. Damit würde allerdings jegliche Kommunikation zwischen LWS und seinen Anwendungen unterbunden. Die Folge wäre, dass sämtliche, angeschlossenen Anwendungen sicher abschalten müssen, und zwar ungeachtet des mit ihnen verbundenen ASILs. Keine der Anwendungen könnte in diesem dann irreversiblen Zustand eine Lenkwinkelinformation mehr bekommen. Außerdem wäre der Kontakt zum LWS von außen komplett gestört und somit sind auch Diagnosemöglichkeiten für den laufenden Fahrzyklus ausgeschlossen. Eine solche Lösung ohne automatische Wiederherstellung, beispielsweise durch zeitlich nur begrenzte Abschaltung, stellt natürlich eine harte Einschränkung in der Verfügbarkeit dar.

Auch eine impulsartige Unterbrechung der Versorgung der Anwendungen mit Lenkwinkeldaten aus dem LWS darf in zumindest sicherheitskritischen Anwendungen nicht unerkannt bleiben. Zur Erkennung und gegebenenfalls angemessenen Reaktion müssen Abschaltsignale per HW entsprechend lang genug ausgegeben werden.

Eine andere Lösung ist, das HW-Abschaltsignal aus dem LWS herauszuführen und den Anwendungen, die auf die hohe Integrität angewiesen sind, direkt verfügbar zu machen. Dadurch können die kritischeren Anwendungen mit ASIL C oder ASIL D selbst entscheiden, was sie mit den weiterhin gelieferten Lenkwinkelinformationen (noch), vielleicht für einen Notlauf, ermöglichen können. Weniger sicherheitsrelevante Anwendungen (ASIL A oder ASIL B) könnten hingegen uneingeschränkt weiter arbeiten. Für diese Lösung müssen in der Praxis natürlich die Kosten für eine zusätzliche Leitung im Fahrzeug gegen die Verfügbarkeit vieler Anwendungen abgewogen werden.

### 7.6.2 Abschaltung durch softwarebasierte Botschaft

Eine weit flexiblere Lösung zur Übertragung von Abschaltinformationen ist die durch digitale Daten und SW. Wie mehrfach erwähnt, generiert das vergleichende Hall-Sensor-IC als Vergleichsergebnis ein digitales Wort. In diesem Wort sollte es konzeptionell nur einen einzigen Wert geben, der für Übereinstimmung steht. Alle anderen Werte darin, inklusive der Werte, die durch zufällige Ausfälle leicht eingenommen werden[78], dienen der Redundanz zur Abschaltung. Bei Verwendung einer Wortbreite von 16 Bit ergibt sich so beispielsweise eine Wahrscheinlichkeit von 1 zu 65535 dafür, dass trotz aufgetretener Fehler nicht korrekt abgeschaltet und stattdessen der eine Wert für Übereinstimmung die

[78] Präferenz- oder Vorzugslagen wie 0 und -1

Anwendungen erreicht[79]. Im Beispiel des praxisorientierten LWS mit µC und Bussystem als Schnittstelle des Moduls nach außen ist dieser für die Anwendungen vordefinierte Wortwert im µC des LWS, der es annehmen und unverändert über das Bussystem an die Anwendungen durchleiten soll, unbekannt. Nur mit diesem Wert kann die Sicherheitsintegrität des LWS von ASIL B im Funktionskanal auf insgesamt ASIL D angehoben werden. Im Normalfall, also bei Übereinstimmung, qualifiziert dieser Wert den ausgegeben Absolutwinkel zum Gebrauch für SZs mit ASIL D. Auch weitere Abstufungen mit weiteren vordefinierten Werten sind vorstellbar, wie eine weitere Patentschrift verdeutlicht [61]. Verschiedenen ASILs zugeordnete Werte im kommunizierten Vergleichsergebnis führen nun nachvollziehbar zur zuvor verwendeten Bezeichnung *ASIL-Qualifier*. Für eine gefährdende Manipulation des ASIL-Qualifiers muss S2 oder der µC im Rechnersystem „raten" oder „würfeln" (systematisch per SW bzw. zufällig per HW). Nur mit dem einen, „richtigen" Wert würde der so überschriebene ASIL-Qualifier in der Empfängeranwendung eine eigentlich beabsichtigte Abschaltung im Fehlerfall verhindern.

Damit MC die Botschaft mit dem ASIL-Qualifier aber nicht falsch, beispielsweise aus einem positiven Regelfall kopiert und dann permanent auch für den Fehlerfall, ins Bussystem aussendet (en: „stuck-at" situation) oder die Botschaft des Hall-Sensor-ICs S2 auf ihrem Weg durch den µC und das Bussystem geschützt bleibt, wird sie bereits in S2 Ende-zu-Ende abgesichert. Per Id, Botschaftszähler und einen über alles kalkulierten und angefügten CRC entsteht auf diese Weise nach Abschnitt 4.7 ein grauer Kanal, das heißt ein Tunnel für den gesamten Übertragungsweg durch Elemente wie SPI, µC und CAN bis zur Anwendung, die die Mechanismen am anderen Ende auswertet und die Daten aus der Sicherheitsschale verwendet. Die Anwendung muss anhand des so empfangenen ASIL-Qualifiers selbst entscheiden, ob und in wie fern Funktionalität abgeschaltet oder degradiert werden muss.

Wegen des oben erwähnten Prinzips der ausfallsicherheitsgerichteten Signale im Konzept werden neben den Daten der Winkelbotschaft auch alle Daten der Qualifier-Botschaft schon auf ihr grundsätzliches Eintreffen hin überwacht. Die empfangenden Anwendungen sind daher darauf eingerichtet, ausbleibende Botschaften zu erkennen, z.B. durch eine zeitliche Überwachung mit definierten Ablaufintervallen (Time-Outs). Natürlich werten die Anwendungen auch die Sicherheitsinformationen der Ende-zu-Ende-Absicherung aus und behandeln sie entsprechend. Andere, zusätzliche Abschaltsignale könnten durch einen für den ausgegebenen Absolutwinkel eines konkreten LWS als ungültig definierten (Diagno-

[79] Die zusätzlichen Mechanismen der Ende-zu-Ende Absicherung greifen erst ab der entsprechenden Provisionierung am sendeseitigen Ende des Übertragungskanals zum Empfänger.

se-) Bereich oder durch zusätzliche Diagnose- oder Statusinformationen bereitgestellt werden. Vor allem aber dienen zur Abschaltung alle Werte eines ASIL-Qualifiers, die nicht für eine Übereinstimmung beim asymmetrisch durchgeführten Vergleich stehen. Jeder erkannte Fehler führt in der von der Vergleichseinrichtung abgesetzten, den ASIL-Qualifier einbeziehenden Anwendung entweder zur Abschaltung der Funktionalität, zu ihrer Einschränkung (Degradation) oder zu einem Alarm bzw. einer Warnung an die Fahrzeuginsassen. Dies geschieht, wie beschrieben, natürlich unabhängig vom Funktionskanal und auf gleicher Integritätsstufe wie für die übrigen Teile des ganzen SMs.

# 8 SICHERHEITSBEWERTUNG DES NEUEN KONZEPTS

In diesem Kapitel geht es nun um die Analyse und Bewertung des vorgeschlagenen Konzepts aus sicherheitstechnischer Sicht. Um die Bewertungen vor einer Verallgemeinerung so konkret und umfassend wie möglich werden zu lassen, orientieren sie sich an der Konzeptanwendung der magnetischen Lenkwinkelerfassung des Kapitels zuvor. In den Teilabschnitten wird insbesondere die Gegenüberstellung zum De-Facto-Standard des EGAS-Konzepts für höchste Funktionssicherheit einer ECU im Automobil von Interesse sein. Andere Ein-Rechner-Lösungen, z.B. mit diversitären, parallelen oder inversen Rechenkanälen im SW-System, sind im anvisierten Bereich unüblich. Daher gibt es kaum Erfahrungen und praxiserprobte Aussagen zur sinnvollen Gegenüberstellung damit bzw. darüber.
Der folgende Abschnitt 8.1 behandelt zunächst die systematisch möglichen Fehler. Abschnitt 8.2 betrachtet die zur Laufzeit möglichen Ausfälle der HW gesondert, insbesondere die mit der Vergleichseinrichtung verbundenen Fehlerquellen selbst. Die Abschnitte 8.3 und 8.4 sollen separiert auf externen Fehlereinfluss bzw. auf den Einfluss der Mechanik eingehen, da diese Einflüsse nicht unmittelbar im Blick der auf elektrische und elektronische Systeme bezogenen ISO 26262 liegen.
Die folgende Tabelle gibt zunächst den Überblick zu sämtlichen Fehlerursachen und Ausfallarten und deren mögliche Beherrschung im Lebenszyklus eines konzeptbasierten Lenkwinkelsensormoduls LWS als die konkrete Beispielanwendung.

Tabelle 8-1: Übersicht der Fehlerursachen und deren mögliche Beherrschung durch das Konzept

| **Fehlerursache** | **Fehlerkategorie** | **Betroffene Technologie** | **Mögliche Sicherheitsfehler- und -ausfallarten** | **Konzeptionell beherrschte Fehler** | **Details in Abschnitt** |
|---|---|---|---|---|---|
| Mensch<br><br>(Entwickler, Tester, Hersteller, Bediener, SW-Werkzeughersteller) | systematisch | SW<br>HW<br>Mechanik<br>Magnetfeld<br>Software-Werkzeuge | Fehler in Spezifikation, Entwurf, Implementierung, Konfigurierung, Fertigung, Kalibrierung oder Fertigung (keine Fehler durch Bedienung, keine Konfigurierung im Betrieb) | falsche Ausgaben oder mangelnde Winkelgenauigkeit, die nicht auf Fehler im Vergleich selbst beruhen | 8.1 |
| Physikalischer und chemischer Einfluss | zufällig im System | HW | Bauelementeausfall | Alle | 8.2 |
| | | Mechanik | Bauteilbruch oder -verschleiß | alle, außer Fehler im Antrieb | 8.4 |
| | zufällig von außen | HW (EME, Strahlung) | Transienter oder permanenter Bauelementeausfall | Alle | 8.2 |
| | | Fremdmagnetfeld | Ergebnisverfälschung | alle, außer ausreichend unwahrscheinliche Konstellationen | 8.3 |

Die Vorgehensweise bei der Analyse und Beurteilung von Ausfällen und Fehlern entspricht dem von der ISO 26262 allgemein geforderten Ansatz vom Abstrakten herunter in die Details (en: top down approach).

## 8.1 Beherrschung systematischer Fehler

In diesem Abschnitt sollen die Fehler systematischer Ursache im Zusammenhang des neuen Sicherheitskonzepts betrachtet werden, und zwar nur qualitativ und nicht quantitativ. Zur systematischen Analyse dienen hier fünf Unterabschnitte. Der erste ist der Entwicklung des Systems, der Mechanik, der Hardware und der Software und den entsprechenden Prozessen dabei gewidmet. Dieser Teil überdeckt die normativ ebenfalls nur qualitativ gebotenen Sicherheitsanalysen zur Betrachtung systematischer Ausfälle und Fehler (nach ISO 26262 Teil 4, 7.4.3 und Tabelle 1 und Teil 6, 7.4.12f), dort beispielsweise durch die Methoden FTA und FMEA. Weitere vier Abschnitte stellen Sicherheitsanalysen zu weiteren Aspekten der Mechanik- und Elektronikimplementierung, zur SW-Implementierung inklusive der SW-Werkzeugketten, zur Verifikation mit Validierung und zu den Fertigungsprozessen dar. Die folgende Tabelle gibt den Überblick zu sämtlichen systematischen Fehlerquellen und Versagensarten im Konzept und deren mögliche Beherrschung.

Tabelle 8-2: Quellen systematischer Fehler und deren mögliche Beherrschung durch das Konzept

| Fehlerquelle | Ursache des Sicherheits-versagens | Konzeptionell beherrschte Fehler | Vergleich mit EGAS-Konzept | Details in Abschnitt |
|---|---|---|---|---|
| Entwicklungs-prozesse für System, HW, SW und Mechanik | Fehler in Spezifikation, Architektur, Entwurf, Schaltung, Konstruktion | falsche Ausgaben oder mangelnde Winkelgenauigkeit, die nicht auf Fehlern der Vergleichseinrichtung selbst beruhen | Der EGAS 3-Layer Aufbau mit Kontrollrechnungen und Rücklesungen ist diffiziler und daher anfälliger | 8.1.1 |
| Bauteil-auswahl und -dimensionierung | Ungeeignete Qualität, Falsche Dimensionierung | | Mehr Bauelemente und Bauteile bei EGAS können wiederum falsch ausgewählt oder dimensioniert werden | 8.1.2 |
| Software-implementierung für µC | Fehler in Programm oder Konfiguration | | Bei EGAS können diese Fehler zur Laufzeit nicht mehr beherrscht werden, weil keine funktionelle Diversität genutzt wird | 8.1.3 |
| Software-werkzeuge | Fehler bei Werkzeugentwicklung und dadurch im Endprodukt | | | 8.1.3 |
| Integration Verifikation Validierung | Verbliebene Fehler im Produkt | | Bei EGAS werden im Betrieb weniger nicht gefundene Fehler aufgedeckt | 8.1.4 |
| Fertigungs-prozesse | Kalibrierung, Fertigung, Montage, Test, ESD | | EGAS ist etwas bauteilintensiver und dadurch anfälliger | 8.1.5 |

### 8.1.1 SICHERHEITSINTEGRITÄT DER ENTWICKLUNGSPROZESSE

Zur Vermeidung systematischer Fehler, die bereits während der Entwicklung eines Produkts wie einem LWS eingebracht werden, muss auch vor allem systematisch vorgegangen werden. Als Basisstandard für eine entsprechende Produktentwicklung inklusive eines SW-Systems ist *Automotive Software Process Improvement and Capability Determination* (ASPICE [40]) oder auch die ISO 15288 (V-Modell; Systementwicklung - Der Lebenszyklus und seine Prozesse) zu nennen. Je klarer und systematischer sich den beteiligten Teammitgliedern die für die Entwicklung definierten Entwicklungsprozesse darstellen, desto weniger Fehler werden ihnen beim Durchlaufen der einzelnen Entwicklungsphasen unterlaufen. Die darüber hinaus gehenden Anforderungen der Norm ISO 26262 hierzu richten sich im Wesentlichen nach der Kritikalität der SZs und ihren zugeordneten ASILs für die jeweilige Funktionalität. Im Falle des Lenkwinkelsensors muss man wegen der Fahrzeugfunktionalitäten ESP[80] und EPS stets von SZs mit dem höchsten ASIL ausgehen, d.h. auch die Entwicklungs- und Hilfsprozesse, -methoden, Arbeitsweisen, Vorlagen, die zum Einsatz kommenden (SW-)Werkzeuge und Analysen müssen den Normanforderungen für ASIL D genügen. Ob nun ein ASIL D für ein SZ nach EGAS-Konzept oder nach einem anderen Konzept realisiert werden soll, die einmal festgelegten Definitionen der Prozesse zum systematischen Vorgehen bei der Entwicklung im Unternehmen werden dabei unterschiedslos dieselben sein und müssen der Norm entsprechend geeignet sein.
Die ISO 26262 unterscheidet nicht die Komplexität des (Sub-)Systems, wie dies bei der Grundnorm IEC 61508 wenigstens mit Typ A für einfache, nicht programmierbare HW und Typ B für komplexere HW mit SW-Technologie der Fall ist. Auch bezüglich Komplexität des entsprechend dem ASIL geplanten Sicherheitskonzepts werden keine dedizierten Anforderungen gestellt. Der für Sicherheit so wichtige Aspekt Einfachheit bezieht sich in der Norm auf die Darlegung und Art von Spezifikationen, Entwürfen und Implementierungen. Trotzdem ist offensichtlich, dass auch die Komplexität eines Sicherheitskonzepts in sich große Auswirkung auf die gesamt betrachtete Funktionssicherheit hat. Um ein technisches EGAS-Sicherheitskonzept mit einem einzigen Rechnersystem/Mikrocomputer auf das Niveau von ASIL D heben zu können, müssen viele einzelne Rechnerüberwachungsfunktionen entwickelt werden, die die Sicherheitsintegrität des Rechners oder der ECU nur in ihrer Gesamtheit und nur indirekt verbessern. Je mehr verschiedene Redundanz- und Kontrollrechnungen durchgeführt und verglichen werden und je engmaschiger diese Kontrollen auch zeitlich sind, desto besser wird die für die eigentliche Funktion genutzte Rechnerintegrität. Das neue Konzept hingegen sichert mit dem ebenfalls extern,

[80] Der Einbau eines ESC (ESP) ist in der EU ab 2014 Pflicht für neue Personenkraftwagen.

aber asymmetrisch angeordneten Vergleich exakt die eigentliche Funktion des Rechnersystems ab, und zwar für jeden berechneten und zur Ausgabe gebrachten Wert. Hierdurch ist das Konzept simpler, mithin leichter zu verstehen und leichter zu realisieren als ein entsprechendes EGAS. Dadurch ist auch die Entwicklung weniger anfällig für systematische Fehler oder Unterlassungen.

Auch ein Sicherheitskonzept mit von vornherein zwei parallelisierten Rechnerkernen, ob als Abwandlung von EGAS oder vollständig redundant[81] und möglicherweise diversitär ausgelegt, wird trotz ähnlichem Funktionsumfang komplexer und auch aufwändiger als die neue Lösung sein. Dies liegt hauptsächlich an den notwendigen Maßnahmen zur Fehlerunabhängigkeit der diversitären Funktionen und Strukturen innerhalb von MC und daran, dass MC nicht wie beim neuen Konzept vollständig zu der einen Seite der funktionellen Diversität gehört. Zur Vermeidung systematischer (SW-)Fehler in MC werden z.B. zwei verschiedene SW-Systeme mit dann angeratenen, zwei verschiedenen SW-Werkzeugketten zu entwickeln sein.

Abgesehen von geringerer Komplexität bietet das neue Konzept gegenüber EGAS mehr Möglichkeiten, die während der Entwicklung eingebrachten Fehler später zur Laufzeit bereits in Prototypen-Prüf- und -Validierungsphasen aufzudecken. Grund dafür ist die weite Teile des gesamten mechatronischen Moduls umfassende, funktionelle Diversität, die am Ende miteinander – extern asymmetrisch angeordnet – plausibilisiert wird.

Nicht unbedingt aufgedeckt werden können dabei allerdings diejenigen Fehler, die systematisch in den kleinen Teil der AAV selbst eingebracht wurden. Zur Vermeidung dieser Fehler muss nach wie vor auf eine vollständige Verifikationsstrategie für die Vergleichseinrichtung gesetzt werden (siehe Abschnitt 8.1.4).

### 8.1.2 Systematische Sicherheitsintegrität der Hardware

Mechatronische Module wie Lenkwinkelsensoren zeichnen sich durch die Kombination mechanischer Komponenten und anderer physikalischer Technologien (z.B. Optik, Akustik, Magnetik) mit Elektrik, Elektronik und auch mit SW aus.

Die Qualität und Sicherheit individueller Mechanik kann meist nur über den (systematisierten) Entwurf und bestimmte Methoden wie Festigkeitsrechnungen, Toleranzrechnungen, Fehlermöglichkeits- und -einflussanalysen (FMEA) und Belastungsanalysen gezeigt werden. Zur Sicherheit werden mechanische Komponenten und Bauteile zudem ihrer Belastung und Anforderung entsprechend überdimensioniert. Der einzige mechanische Bereich im Konzeptbeispiel des LWS-Moduls, der nicht durch funktionelle Diversität abge-

[81] Z.B. auch als sogenannter Lockstep-Mikrocontroller auf einem einzigen Silizium-Die

deckt ist, ist die Verbindung des Antriebsrades mit der Lenkspindel, das Antriebsrad zum Antrieb der beiden kleinen Messräder und die Verbindung des Moduls als Stator mit der Lenksäule. Bei einem LWS muss über den Mitnehmer und die Zahnräder jedoch keine nennenswerte Kraft übertragen werden, sodass hier besser mehr Aufwand bei der Präzision zur Verbesserung der Genauigkeit investiert werden sollte. Neben angemessenen Maßnahmen zur Unterlastung (durch Überdimensionierung) kann dagegen auf rein mechanisch angelegte SMs verzichtet werden.

Elektronische und mikroelektronische Unterstützung im Automobil hingegen muss sich bezüglich Sicherheit, wie in Abschnitt 5.1 beschrieben, den Anforderungen bestimmter Sicherheitsnormen stellen. Neben den bereits im vorherigen Abschnitt 8.1.1 auch für die HW geltenden Anforderungen an die Entwicklungsprozesse und -methoden muss zur Vermeidung systematischer Fehler bei der HW-Entwicklung insbesondere auf die richtige Auswahl und Dimensionierung der Bauelemente geachtet werden.

Für die Qualität, auf die die Sicherheit üblicherweise aufbaut, gelten als internationale Standards in der Automobil- und -zulieferindustrie die auf die ISO 9001 [75] aufbauende ISO 16949 (Automotive Quality Management) [76] für Prozesse und die AEC Q (parts reliability & quality) für die Qualität aktiver und passiver Bauelemente. Für Ausfallraten und die Zuverlässigkeit einzelner Bauteile gelten Normen wie die ISO 62380 (UTE-C80810), die DIN 61709 (SN 29500), die MIL HDBK 217 F notice 2 oder die RAC HDBK 217 Plus und einige andere. Die ISO 16750 (Road vehicles - Environmental conditions & Testing) beispielsweise kann bezüglich Fehler durch die Umwelt (z.B. elektromagnetischer Einflüsse und Störungen) herangezogen werden.

Bei der Auswahl und Dimensionierung der Bauelemente ist neben allgemein angemessener Qualität auf angemessene Werte, Toleranzbereiche, Lebenserwartung, Festigkeiten gegen elektrische Spannung, elektrostatische, (elektro-)magnetische Einflüsse und auf Temperaturbereiche zu achten.

Auch gegen die systematischen Fehler in diesem Bereich ist das neue Konzept gegenüber einem EGAS-Konzept robust, weil die in der Funktion g gegebene funktionelle Diversität sämtliche elektronischen Bauelemente bis auf die Vergleichseinrichtung selbst überdeckt. Sollte die Vergleichseinrichtung durch diskrete HW oder einen entsprechenden Analogbaustein realisiert werden, käme es für diesen Abschnitt also vor allem auf die richtige Wahl und Dimensionierung des Bausteins oder der diskreten Bauelemente an.

Bei der im (Kontroll-)Sensor S2 vorgesehenen, digitalen Lösung für den abschließenden Vergleich des neuen Konzepts muss das ganze IC als Bauelement den Anforderungen der ISO 26262 für ASIL B(D) genügen. Der kleine Teil der digitalen Vergleichseinrichtung

darin muss korrekt für einen eingeschränkten Vergleichstoleranzbereich spezifiziert sein. Die Wahrscheinlichkeit dafür, dass eine unter systematischen Fehlern leidende Vergleichseinrichtung mit ihrer Ausgabe auch für die zur Aufdeckung bestimmten Fehler eine Übereinstimmung feststellt oder schlicht anzeigt, ist angesichts tausender anderer möglicher Werte als vernachlässigbar gering einzuschätzen. Nur dieser einzige Fall wäre sicherheitsrelevant gefährlich und kann angesichts einfacher Prüfungen vor dem Einsatz des (Sub-)Systems im Feld ausgeschlossen werden.

### 8.1.3 SICHERHEITSINTEGRITÄT DER SOFTWARE

Das Programm im SW-System des Mikrocontrollers MC muss im Wesentlichen die zwei linearen, zu einander diversitären Funktionen $a = f1(e)$ und $e' = (g \circ \overline{f1})\,(a)$ leisten.
Neben den in Abschnitt 8.1.1 bereits genannten Aspekten bezüglich systematisch eingebrachter Fehler müssen auch die zur Entwicklung und Verifikation zum Einsatz kommenden Hilfsmittel kritisch zu ihrer Eignung beurteilt werden. Dies gilt wegen der charakteristischen Komplexität und Intransparenz natürlich insbesondere für SW-Werkzeuge. Die korrekte Funktion solcher computerbasierten Werkzeuge, die ja grundsätzlich hilfreich sind und generell vom Stand der Technik für mehr Sicherheit gefordert werden, hängt wieder vom Menschen ab, der bei der Entwicklung solcher Werkzeuge durch Irrtum mehr oder weniger Fehler einbringt. Je nach Einsatzfall für ein Werkzeug können auch mehr oder minder gravierende, sicherheitsbezogene Fehler in das Produkt eingebracht werden oder, bei Werkzeugen zur Verifikation und zum Test, im Produkt unerkannt verbleiben. Besonders Werkzeuge zur Übersetzung und zum Bau eines SW-Systems[82], die sogenannten Toolketten, können sich schnell unerkannt gefährlich im Betrieb des Systems bemerkbar machen, weil darin enthaltene Fehler das Produkt und sein Verhalten direkt verändern.
Systematische Fehler bei der Umsetzung der Funktionen in SW können auch mit der Wahl der Programmiersprache und entsprechenden Programmierrichtlinien reduziert werden. Aus Lesbarkeits- und Übersichtsgründen soll für höhere Integrität eine grafische Notation oder eine geeignete Hochsprache zum Einsatz kommen, die allerdings einen eingeschränkten, einfachen Befehlssatz haben soll. Ein auf die Grundelemente reduziertes C nach ANSI-Standard könnte für komplexere Implementierungen bereits problematisch sein und soll in jedem Fall Kodierregeln wie z.B. MISRA-C:2012 folgen. Besser geeignet sind spezielle und ausgereifte Hochsprachen wie RTE[83] oder HI-PEARL[84]. Allzu neue Sprachen bzw.

[82] Compiler, Linker, Builder, Programmer, aber auch z.B. Konfigurationsmanager
[83] Real-Time Euclid, die erste zuteilbarkeitsanalysierbare Echtzeitprogrammiersprache
[84] High Integrity – Process and Experiment Automation Realtime Language mit Vorläufern seit Ende der 1960er Jahre

Versionen von Sprachen wie PEARL2020, wenn auch speziell für modernste Belange sicherheitsgerichtet ausgelegt, sollten für die Anwendung im realen Leben des Straßenverkehrs nicht ohne weitere besondere Vorkehrung[85] eingesetzt werden, da auch die entsprechenden Übersetzungswerkzeuge (s.o.) erst eine gewisse Reife haben und ein auf Langzeiterprobung gesetztes Vertrauen genießen sollten.

Die für einen LWS bereits in den Abschnitten 7.2 - 7.4 und eventuell mit Abschnitt 7.5 für die Vergleichseinrichtung spezifizierten Softwareaufgaben sind recht überschaubar, wenig komplex und leicht zu implementieren. Eventuell trotzdem eingebrachte Fehler können durch den asymmetrisch und extern angeordneten Vergleichsmechanismus bzw. durch die AAV sehr bald aufgespürt und noch während der Entwicklungsphasen beseitigt werden.

Das neue Konzept bietet aufgrund seiner funktionellen Diversität, die das geplante SW-System zur Umsetzung der beiden oben genannten Funktionen im Rechnersystem und auch die Firmware für die Trigonometriefunktionen der beiden Sensoren komplett einschließt, auch hier eine zur Anhebung von ASIL B auf ASIL D geeignete Absicherung. Bei einem entsprechenden EGAS-Konzept würden auf Ebene 2 die erste Funktion $a = f(e)$ parallel und möglicherweise identisch gerechnet und das Ergebnis auf Korrektheit geprüft. Systematische Fehler in der für die Ausgabe relevanten Berechnung werden somit zur Laufzeit nicht mehr auffallen. Auch wenn in Ebene 1 bei EGAS auf Basis des zweiten Sensors S2 eine zweite Funktion $a'=g(e_2)$ gerechnet und zur Absicherung parallel auf Ebene 2 nachgerechnet würde, müssten systematische Fehler darin nicht unbedingt auffallen und erkannt werden können. Selbst ein Kreuzvergleich der Ergebnisse $a$ mit $a'$ könnte wegen eines systematischen Fehlers in beiden, analog gerechneten Zweigen unter bestimmten Umständen noch zu positiven Vergleichsergebnissen führen, wenn z.B. fehlerbedingte Abkürzungen genommen werden und 1 mit 1 oder 0 mit 0 verglichen würde oder der Vergleich selbst nicht funktioniert.

Das Konzept zur Prüfung einer Vergleichsgröße $e'$ unter Nutzung der Ausgabegröße $a$ stellt damit gegenüber einem EGAS-Konzept verbesserte Sicherheit dar.

### 8.1.4 Verifikation und Validierung der Modulfunktion

Zu einer Verifikation (und Validierung) eines technischen Produkts nach Sicherheitsstandard ISO 26262 gehören im Wesentlichen Prüfungen verschiedenster Methoden und auf allen verschiedenen Ebenen der Integration (vgl. auch [77]). Zur Verifikation von SW werden auf diesen Testebenen in der Regel manuelle Inspektionen des Quelltexts, stati-

[85] Gerade PEARL 2020 ist mitunter darauf ausgerichtet, leicht rückübersetzt werden zu können und Maschinenprogramme damit verifizieren zu können.

sche Codeanalysen[86], SW-Unittests, SW-Integrationstests, SW-Systemtests, SW-in-HW-Integrationstests, Mechatronikmodultests, Umwelteinflusstests usw. durchgeführt. Einschlägige Beweisverfahren werden in dieser Norm weder genannt noch gefordert, wenn man einmal von Vergleichstests von Simulationsergebnissen zwischen Modell und Code (en: back-to-back comparison test) für SW absieht, sofern diese Methode wegen ihrer Unvollständigkeit überhaupt als Beweisverfahren gelten kann.

Die Implementierung eines SW-Systems per Hochsprache könnte auch unter symbolischer Ausführung mit einem Werkzeug wie Polyspace für die Sprache C leicht analysiert werden. Die einzelnen Befehle und bedingten Sprünge im Programm werden symbolisch mathematisch umgesetzt und mit ihren jeweils möglichen Datenbereichen vollständig durchgerechnet. Dadurch können bereits statisch die meisten Fehler z.B. bezüglich Speicherbereichszugriffen, Initialisierungen, Parameterübergaben, Schnittstellen, Kontroll- und Datenfluss, Verzeigerung und sogar etliche Laufzeitfehler wie mögliche Division durch Null im Programm aufgedeckt und eliminiert werden. Auf diese auch die Implementierung eines SW-Systems verifizierende Weise kann auf praktikable Art ein mathematischer Beweis der Richtigkeit eines Programms vermieden werden. Normativ wird dieser zumindest für die maximal zu erreichende Integrität der Stufe ASIL B ohnehin nicht erfordert.

Wegen des Ausschlusses von Nebenläufigkeit im Programm kann auf eine Verifikation mittels temporaler Logik verzichtet werden. Eine Zuteilbarkeitsanalyse für Rechenzeiten oder auch z.B. Schnittstellen-Ressourcen (SPI zu den Sensoren S1 und S2) kann deshalb ebenfalls entfallen. Jegliche fehlerbasierten Abbrüche im Programmablauf können als sicher betrachtet werden, da in solchen Fällen auch eine entsprechende Bewertung durch die externe Vergleichseinrichtung ausbleiben und damit per Definition ein sicherer Zustand eingenommen werden würde.

Ziel aller Maßnahmen zur Verifikation und Validierung eines Systems und insbesondere eines softwarebasierten Systems ist das Aufspüren möglichst aller darin entstandenen, systematischen Fehler. Leider beweisen Tests, insbesondere die immer unvollständigen Tests von SW, nur die Existenz von Fehlern und nicht die Korrektheit eines Programms.

Und natürlich können auch die übrigen Prüfungen und sonstigen Maßnahmen zur Verifikation (systematisch) selbst versagen. Ursachen dafür können zum Beispiel Fehler oder Auslassungen im Prüfumfang, bei der Methodik oder auch bei Fehlern in den softwarebasierten Verifikationswerkzeugen sein. Ein Werkzeug zur Durchführung automatisierter

[86] z.B. mit Software-Werkzeugen wie IAR-Compilern, Lint, LDRA oder QAC zur Übereinstimmung mit MISRA-C:2012 für die Hochsprache C

Prüfungen, das beispielsweise bestimmte oder gar sämtliche Testfälle unter gewissen Umständen als fehlerlos durchlaufen markiert, macht alle betreffenden Prüfungen nutzlos.
Zur Verifikation käme – ungeachtet, ob modellbasierte Entwicklung mit Codegenerierung oder eine hochsprachliche Implementierung bevorzugt wird – auch die Rückwärtsanalyse mit Rückübersetzung des Maschinenprogramms in Frage. Unter Umständen können hier SW-Werkzeuge wie PVS[87] zum Einsatz kommen. Natürlich können auch bei dieser Verifikationsmaßnahme systematische Fehler nicht generell ausgeschlossen werden.
Mit dem neuen Konzept ergibt sich jedoch der Vorteil, dass sämtliche Messungen in den Sensorbausteinen und die Berechnungen im Mikrorechnersystem zur Laufzeit durch den Vergleichsmechanismus verifiziert werden. Ähnlich wie bei der Rückwärtsanalyse wird dabei ein diversitärer Weg genutzt. Während bei der Rückwärtsanalyse die Eingangsspezifikation der geplanten Funktion mit dem diversitär erbrachten Resultat der Rückübersetzung (Re-Engineering) verglichen wird, werden im neuen Konzept die zur Ausgabe bestimmten Rechenergebnisse diversitär auf ein diversitär ermitteltes Messergebnis zurückgeführt und mit diesem verglichen. Eine Sicherheitslücke könnte sich dabei auch hier, allerdings ausschließlich beim verifizierenden Vergleich selbst ergeben. Mit einer korrekt verifizierten Vergleichseinrichtung V (und der Fehlerbehandlung bzw. dem Abschaltpfad) ist demnach gleichzeitig der Rest des Systems bzw. des Sensorikmoduls verifiziert und seine korrekte Funktion belegt.
Der Vergleich in der Vergleichseinrichtung im Konzept und auch die absichernden CRC-Berechnungen sind algorithmisch trivial, wie wir in Abschnitt 7.5 gesehen haben. Diese Teile können leicht und müssen nach ihrer konkreten Realisierung in einem Entwicklungsprojekt einmalig verifiziert werden – sofern nicht bereits fertig verifizierte und qualifizierte Bibliotheken dafür verfügbar sind und zum Einsatz kommen.
Gegenüber dem EGAS-Konzept beschränkt sich die gesamte Verifikation beim neuen Konzept, zusammenfassend gesagt, auf die korrekte Funktion der asymmetrisch angeordneten Vergleichseinrichtung (AAV) mit seinen Ausgabepfaden.

### 8.1.5 Sicherheitsintegrität der Fertigungsprozesse

Auch während der Fertigung eines sicherheitsgerichteten Produkts wie einem Sensorikmodul können systematisch Fehler einfließen, von denen nachher im Betrieb Gefahren ausgehen können. Ob in der Fertigungslinie der HW, bei der Logistik und Selektion der HW- und SW-Komponenten, -varianten und -versionen, bei der manuellen Montage oder im Bandendetest, fast überall können sich auch sicherheitsrelevante Fehler einschlei-

[87] Prototype Verification System von SRI

chen. Hier unterscheidet sich das neue Konzept nicht grundsätzlich von anderen Konzepten wie dem altgedienten EGAS-Sicherheitskonzept. Trotzdem ist beim vorgestellten Konzept der wirklich sicherheitsempfindliche Teil des ganzen Systems wieder auf die Vergleichseinrichtung und ihre Ausgabepfade beschränkt. Eventuelle Vorschädigungen von mechanischen Bauteilen oder elektronischen Bauelementen, z.B. durch mechanische, chemische, thermische oder auch magnetische Misshandlung oder durch ESD, sind sicherheitstechnisch nicht relevant, wenn sie den einen oder den anderen diversitären Pfad im System betreffen. Diese Pfade überdecken allerdings die weitesten Signalstrecken im Modul, sodass bei der Prozess-FMEA für einen konkreten LWS nur der Geberantrieb (Mitnahme und Antriebszahnrad) und am anderen Ende das die Vergleichseinrichtung enthaltende Bauelement als sicherheitskritisch und zur hinreichenden Absicherung verbleiben und mit entsprechenden Maßnahmen versehen werden müssen.

## 8.2 Beherrschung zufälliger Ausfälle der Hardware

Mikroelektronische Ausfälle während der Lebenszeit der HW sind zufällige Ausfälle, die entweder dauerhaft oder transient auftreten. Die Normen für funktionale Sicherheit betrachten die aus zufälligen HW-Ausfällen resultierenden, gefährlichen Fehler neben allen systematisch möglichen Fehlern bekanntermaßen nur als einen Teil der zu minimierenden Risiken. Die Analyse dieser durch Physik und Zufall entstehenden Fehler und Risiken, die sich im Gegensatz zu den systematisch entstandenen Fehlern gleichmäßig stetig einem sicherheitsbezogenem Schadensausmaß zuordnen lassen, soll die Aufgabe des vorliegenden Abschnitts sein. Die gewählte Form dieser Analyse zur Beurteilung stellt eine sehr vereinfachte Form der in der ISO 26262 für ASIL D geforderten Sicherheitsanalysen zur HW (Teil 5, 7.4.3.) dar. Es werden dort quantifizierbare, induktive und deduktive Analysen des Entwurfs und die Ermittlung zugehöriger Metriken, beispielsweise mit den Methoden FTA und FMEA erläutert, die sehr ins Detail gehen. Auf dieses Detail muss aber wegen des lediglich konzeptionellen Charakters des hier behandelten (Sub-)Systems verzichtet werden. Eine gar zur Quantifizierung notwendig komplette Stückliste existiert dafür noch nicht. Vor allem aber ist der Verzicht auf z.B. eine detaillierte FMEDA an dieser Stelle wegen der Überschaubarkeit des Konzepts und eines konzeptbasierten Systems und wegen der pauschalen Kategorisierbarkeit als auch guter Zusammenfassbarkeit aller zufälligen Ausfälle gerechtfertigt.

Die folgende Tabelle 8-3 gibt zunächst einen Überblick über die möglichen elektrotechnischen Ausfälle und Fehlerquellen samt möglichen SMs und Angaben zu jeweils entsprechender Bewertung. Die nachfolgenden Unterabschnitte 8.2.1 bis 8.2.3 sind dezidiert den

einzelnen Baugruppen „Sensorbauelemente“, „Rechnersystem“ und der Vergleichseinrichtung „AVV“ gewidmet, um dort detailliert die jeweiligen Ausfallmöglichkeiten im Vergleich mit EGAS zu erörtern.

Tabelle 8-3: Zufallsfehlerquellen der Elektronik und deren mögliche Beherrschung durch das Konzept

| **Fehlerort Ausfall in** | **SM zur Fehlerbeherrschung gegen** | | **Gegenüberstellung EGAS gegen SPFs** |
|---|---|---|---|
| | **SPFs** (SPFM ist ≥ 99%) | **LFs** (LFM ist ≥ 90%) | |
| Hall-Sensor (S1, IC1) | AAV | Integrierte Diagnose-mechanismen | Parallel berechneter Vergleich mit S2 |
| Mikrocontroller (MC, IC2) | AAV | Integrierte Diagnose-mechanismen | Ebene 2 mit Parallel-rechnungen |
| Energiever-sorgung mit Filter u. Span-nungsregler | AAV | Überwachung der Spannung durch S1 und S2, die selbst spannungsfest sind | (keine Angaben) |
| Takterzeugung für MC | AAV | S1 als Fensterwatchdog mit unabh. Zeitbasis | Zusätzlich externer Fensterwatchdog |
| Hall-Sensor (S2, IC3) | AAV | Integrierte Diagnose-mechanismen | Parallel berechneter Vergleich mit S1 |
| Vergleichs- und Abschalt-einrichtung in S2 (IC3) | Der richtige ASIL-Qualifier wird bei einem Ausfall sehr unwahr-scheinlich getroffen und noch dazu richtig Ende-zu-Ende abgesichert | In S2 integrierte Diag-nosemechanismen und Test durch MC beim Start | Ausfälle für Vergleiche in Ebene 2 werden durch Mechanismen in Ebene 3 beherrscht, jedoch zeitlich und wertmäßig nicht direkt |
| Bus-Transceiver | Ende-zu-Ende-Absicherung MC Ende-zu-Ende-Absicherung S2 | Ende-zu-Ende-Absicherung MC | Ähnlich, aber Lücke bei Übergabe der Werte innerhalb der Software |

Die sicherheitstechnisch wesentlichen, elektronischen Komponenten im Einsatz des Konzepts für ein komplettes Sensormodul sind die Sensorbauelemente S1 und S2, das Rechnersystem MC und die in einem oder beiden Sensorbauelementen integrierte Vergleichs- und Abschalteinrichtung V. Zur Betrachtung dieser drei Bereiche sollen die folgenden drei entsprechenden Unterabschnitte dienen. Der ganze Bereich der elektronischen Schnittstelle für z.B. CAN oder Flexray in das Fahrzeugsystem, zu dem auch der passive Bus-Transceiver und die in MC integrierte Schnittstellenperipherie gehören, bilden bereits einen Ende-zu-Ende abgesicherten, grauen Kanal. Sämtliche Ausfälle darin werden an der Empfängerseite aufgedeckt und sicherheitstechnisch beherrscht. Beim EGAS-Konzept könnte der Bereich zwischen abschließender Plausibilisierung der Ausgabewerte und ihrer Übergabe zur Ende-zu-Ende-Absicherung und anschließender Kommunikation eine Sicherheitslücke darstellen. Ausfälle der Rechnerhardware genau in diesem Bereich werden unter Umständen nicht oder nicht rechtzeitig erkannt. Das Rechnersystem kann je nach FTTI nicht rechtzeitig reagieren, wenn das im Konzept eventuell geplante Zurücklesen der Werte vom Systembus oder vom Empfänger zu viel Zeit beansprucht.

### 8.2.1 HARDWARESICHERHEITSINTEGRITÄT DER SENSORBAUELEMENTE

Einzelne Ausfälle und Fehler in einem der Sensorbauelemente (Hall-Sensor-ICs), die das Potential zur unmittelbaren Verletzung eines SZs hätten, können durch die Vergleichseinrichtung des neuen Konzepts erkannt und beherrscht werden. Wegen des unabhängigen, zumindest für den ersten Sensorbaustein S1 externen Vergleichs sollten 99%[88] oder mehr aller HW-Ausfälle sicher bleiben oder in einen sicheren Zustand geführt werden können.
Im System mit EGAS-Konzept würden diese Ausfälle nach externer, im Rechnersystem parallel laufender Umrechnung zu einem Absolutwinkel und anschließendem Vergleich mit hoher Diagnosedeckungsrate auffallen und somit ebenfalls beherrscht werden können.
Untersucht werden müssen nun noch Ausfälle in S1 (und S2), die in Kombination mit anderen Ausfällen im System gefährlich werden könnten. Dies beträfe zum Beispiel Ausfälle in Teilen des Sensorchips, die – abgesehen von der Vergleichseinrichtung, die später separat betrachtet wird – z.B. weiterer Fehlererkennung dienen. Solche zusätzlichen Bereiche (integrierte SMs oder -maßnahmen gegen SPFs und LFs) sind jedoch für das Konzept mit Vergleichseinrichtung und ASIL D nicht notwendig, solange von einer integeren Vergleichseinrichtung ausgegangen werden kann, die sämtliche Fehler beherrscht.
Nur für den Fall, dass z.B. die Vergleichseinrichtung im System bereits erkannt ausgefallen ist und sich das System im Notlauf ohne Sensorredundanz befindet oder dass für manche Items von vornherein nur S1 referenziert wird (siehe Abschnitt 6.2), wird eine (Rest-) Integrität der HW wie z.B. für ASIL B benötigt, die dann weitere SMs im Sensorbaustein erforderlich macht. Prinzipielle Unterschiede zur Situation beim EGAS-Konzept bestehen an dieser Stelle dann nicht.
Im Folgenden soll am Beispiel des in Abschnitt 5.2.3 vorgestellten Hall-Sensor-ICs MLX90363 aufgezeigt werden, welche Sicherheitsmechanismen und –maßnahmen zur Verbesserung der HW-Integrität auf Stufe ASIL B zum Ansatz gegen SPFs und auch LFs kommen. Der MLX90363 besitzt nämlich bereits eine Vielzahl eingebauter Eigenschaften zur Selbstdiagnose und Fehlervermeidung, an denen die Beherrschung der unterschiedlichen Fehlerarten gut verdeutlicht werden kann.
Während die einmalig beim Start durchgeführten Diagnosen grundsätzlich nur latente Fehler (LFs) und jenseits von FTTIs vermeiden, eignen sich zyklisch permanent ausgeführte Diagnosen und auch bestimmte, permanent wirksame Maßnahmen in Entwurf und Konstruktion zur Beherrschung von Fehlern mit Potential zu SPFs. Voraussetzung zum Ansatz ihrer Beherrschung ist neben der Erkennung natürlich immer auch die Gewährleistung für einen sicheren Zustand in der Folge der Fehleraufdeckung.

[88] Normativ wird unter den gegebenen Umständen der Ansatz von „high“ bzw. 99% als DC zugestanden.

Die folgende Tabelle aus [63] listet die diagnostischen Maßnahmen gegen interne und externe Fehlerfälle des genannten Hall-ICs mit den entsprechenden Fehlerreaktionen auf. Der Entwurf und die Implementierung all dieser SMs ist darauf ausgerichtet, dass innerhalb von 30 ms über 90% aller Teile mit Potential zur Verfälschung von Messwerten entweder als korrekt oder aber als defekt angezeigt werden können. Dieses Zeitintervall und diese DC passt zu den typischen Fahrzeugfunktionalitäten mit ASIL B, die von Lenkwinkeldaten auf Stufe ASIL B abhängig sind.

Tabelle 8-4: Beherrschung zufälliger Fehler durch Ausfälle in der HW des MLX90363

| **Diagnostische Maßnahme** | **Fehlerreaktion** | **Bit** | **Bemerkung** |
|---|---|---|---|
| RAM March C- 10N Test | Modus sicherer Zustand | D0 | nur beim Start |
| Watchdog Selbstüberwachung | Modus sicherer Zustand | D1 | nur beim Start |
| ROM 32 bit Prüfsumme | Modus sicherer Zustand | D2 | |
| RAM Test (fortlaufend) | Modus sicherer Zustand | D3 | |
| CPU Test | Modus sicherer Zustand | D4 | auf Register Test beschränkt |
| EEPROM Prüfsummentest (8 bit CRC) | Modus sicherer Zustand | D5 | |
| EEPROM Hamming Code DED (Dual Error Detection) | Modus sicherer Zustand | D6 | |
| EEPROM RAM Cache Fehler Test | Report 1) | D7 | |
| ADC Test mit Referenz und Prinzip | Report | D8 | |
| Analogkettenversatzüberwachung | Report | D9 | |
| Spannungsversatzüberwachung | Report | D10 | |
| (Analogverarbeitungsüberwachung, nicht implementiert) | Report | D11 | |
| Bz Sensitivitätsüberwachung | Report | D12 | |
| Bx Sensitivitätsüberwachung | Report | D13 | |
| By Sensitivitätsüberwachung | Report | D14 | |
| Temperatursensorüberwachung | Report, Temperaturwert auf EE_T35 gesetzt | D15 | |
| Temperatur > 190° (± 20°) Temperatur < -80° (± 20°) | Report, Wert der Sättigungstemperatur | D16 | externer Fehler |
| Feldstärke zu hoch (Norm1 > 99% ADC Spanne) | Report | D17 | externer Fehler |
| Feldstärke zu schwach (Norm1 < 20% ADC Spanne) | Report | D18 | externer Fehler |
| ADC Amplitudenbegrenzung | Report | D19 | externer Fehler |
| Spannungsversorgungstest (VDD) und Reglerüberwachung (VDEC) 2) | Report | D20 | externer Fehler |
| Stromüberwachung | Report | D21 | |
| Stromquellenüberwachung | Report | D22 | |
| Hall-Platten-Stromüberwachung | Report | D23 | |
| Programmablaufüberwachung | Modus sicherer Zustand | - | |
| Überwachung der Schreib- u. Lesezugriffe außerhalb physikalischer Speichergrenzen | Modus sicherer Zustand | - | |
| Überwachung Stack Überlauf | Modus sicherer Zustand | - | |
| Überwachung Schreibzugriff auf geschützte Bereiche (IO und RAM-Zellen) | Modus sicherer Zustand | - | |
| Überwachung unauthorisierter | Modus sicherer Zustand | - | |

| | | | |
|---|---|---|---|
| Einstieg in den “SYSTEM” Modus | | | |
| Überwachung SPI Schutzfehler | NTT Telegramm 3) | - | |
| Watchdog Timeout | Reset 4) | - | |
| Schwingkreis Frequenzmessung (Protokollerweiterung zur genauen Messung) | n/a | - | Diagnose ausgehend vom Master |
| VDD > 6,5V Abschaltung | Master-In-Slave-Out Leitung wird hochohmig | - | 100% hartkodierte Detektion; Keine Kommunikation mehr möglich |

1) Der Master registriert einen erkannten Fehler mittels der Bits E0 und E1 in den Regulär-Telegrammen oder über die Bits Dx in den dedizierten Diagnose-Telegrammen.
2) Diese Diagnose soll in der 3,3V Anwendung nicht verwendet werden ($V_{DD} = V_{DEC}$).
3) Auf das Telegramm NTT (Nothing to transfer) folgt immer noch ein Fehlertelegramm.
4) Rücksetzen hat den gleichen Effekt wie ein Neustart (POR – Power On Reset): das nächste ausgehende Telegramm ist deshalb das Telegramm mit dem OpCode „Ready“.

Vor dem Übergang in den normalen Betriebsmodus des ICs findet beim Start des Bausteins zunächst ein eingebauter Selbsttest (en: built-in self test, BIST) statt, bevor im Rahmen der Initialisierung der Speicher, die Ports, die serielle Schnittstelle SPI und sonstige Peripherie auf definierte Werte eingestellt werden. Daraufhin wird die automatische Analogverstärkung eingestellt und die Temperaturermittlung (mit zwei integrierten, redundanten Temperatursensoren) gestartet. Mit dem nächsten Schritt werden erstmalig die Digitalteildiagnosen und alsdann die Analogteildiagnosen ausgeführt. Diese werden später in einem Hintergrundprogramm auch kontinuierlich durchlaufen. Zuletzt wird die serielle Schnittstelle nach außen aktiviert und für die Anforderung eines SCI/SPI-Masters freigegeben. Der ganze Startvorgang vom Anlegen der Stromversorgung bis zum regulären Betrieb des Bausteins ist in Abbildung 8.1 grafisch dargestellt.

Der Zweck der in der Tabelle 8-4 genannten Betriebsart „Modus sicherer Zustand“ ist zweierlei. Zum einen soll die Sicherheitsintegrität dadurch erhöht werden, dass die Winkelberechnung und die Ergebniskommunikation blockiert wird, wenn ein kritischer Fehler erkannt wird, wie z.B. ein Fehler beim Watchdog, eine unplausible CRC Prüfsumme oder ein Fehler im Programmablauf der Firmware. Zum anderen soll immer noch die Ursache des Ausfalls nach außen übermittelt werden können, damit eine gegebenenfalls fällige Entscheidung zur Sicherheitsabschaltung auch an höherer Stelle außerhalb des ICs getroffen werden kann.

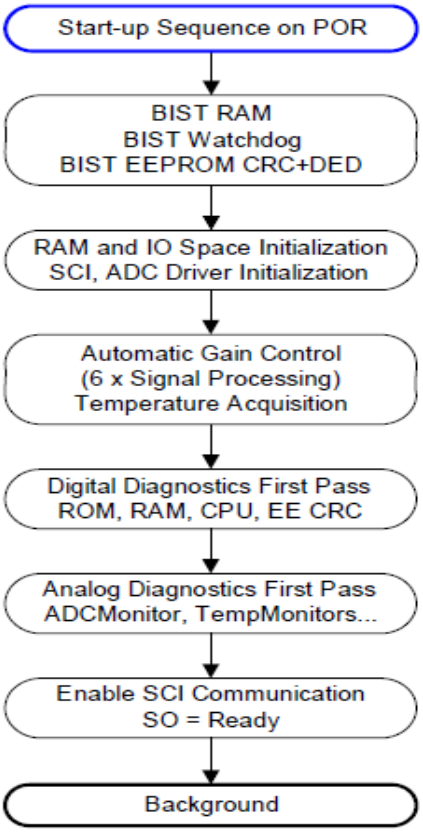



Abbildung 8.1: Firmware Startsequenz [63]

In dieser sicheren Betriebsart wird der Analogteil des Bausteins deaktiviert und der Digitalteil des Bausteins wartet auf Kommunikationsanforderungen des Masters, bis dieser über ein Telegramm ein Rücksetzen des Bausteins anfordert. Die Dauer dieser Betriebsart ist längstens 100 ms lang, bis sich der Baustein über seinen in diesem Modus auf ein Zeitfenster von 100 ms erweiterten Watchdog von selbst zurücksetzt.
Für den “Modus sicherer Zustand” des Bausteins gilt außerdem:

- Nur die SPI Treiberstufe und der Kommunikationsorganisierer bleiben aktiv. Die einzigen möglichen Kommandos des Masters sind die zum
- Zurücksetzen des Bausteins (sciREBOOT) und
- Aktualisieren der CRC Prüfsumme (sciUpdateCRC).
- Als Reaktion auf alle anderen Kommandos des Masters sendet der Baustein das Telegramm SPI_ERROR mit den Diagnosedetails.
- Die Diagnosen des Analog- und Digitalteils wie auch das Hintergrundprogramm sind angehalten.

Der Zustand „Modus sicherer Zustand” des Bausteins wird eingenommen, wenn

- ein kritischer Fehler während der Initialisierung erkannt wird (RAM BIST, WD BIST, ROM Prüfsumme, EEPROM CRC),
- ein kritischer Fehler während der Digitalteildiagnostik im Hintergrundprogramm erkannt wird (RAM Test, ROM Test, EEPROM CRC),
- bei einer Ausnahmebehandlung durch Systemunterbrechungen (Stapelüberlauf, ungültige Adresse, Schutzfehler, Programmfehler),
- ein Programmablaufkontrollfehler in der Firmware erkannt wird.

Die letzte Zeile der Tabelle 8-4 weist auf einen nicht konfigurierbaren Hardwaremechanismus hin, mit dem die Versorgungsspannung VCC (Sekundärspannung) gegen Spannungen größer 6,5 V hin überwacht wird. Der Baustein signalisiert Überspannung an einem seiner Kontakte und ist selbst bis 18 V spannungsfest ausgelegt. Das Signal kann zur Abschaltung sicherheitsrelevanter Bauelemente wie dem Mikrocontroller genutzt werden, sodass durch diesen Mechanismus z.B. auch ein durchlegierter Spannungsregler in der Energieversorgung aller Komponenten des Sensormoduls ungefährlich bleiben kann.
Zusätzlich erhöhen viele andere konstruktive Maßnahmen im Entwurf des Bausteins seine Integrität gegen alle Arten zufällig auftretender Fehler. Hier seien zum Beispiel eine Redundanz bei den Hall-Platten, eine differentielle Analogwertverstärkung und -übergabe in den Digitalteil oder die auch sonst üblichen Mehrfach-Vias zur Durchleitung von Signalen auf andere Siliziumschichten im Die[89] genannt.

### 8.2.2 HARDWARESICHERHEITSINTEGRITÄT DES RECHNERSYSTEMS

Wie beim EGAS-Konzept besteht das Rechnersystem beim neuen Konzept mit asymmetrisch extern angeordnetem Vergleich im Wesentlichen aus einem einzigen Mikrocomputer und darin einem einzigen Rechenkern (CPU). Dies ist die Zielvorgabe für klassische[90] ECUs in der Automobilbranche, nach Möglichkeit sogar auch unter höchsten Sicherheitsanforderungen auf Stufe ASIL D. Der konservative und naheliegende Weg zu einer mit ASIL D vergleichbaren Hardwaresicherheitsintegrität mit zwei redundant zueinander geschalteten Rechnersystemen, die sich gegenseitig überwachen, soll wegen seines Aufwands als Standardlösung vermieden werden. Das als EGAS bekannte Sicherheitskonzept baut wie das hier vorgestellte Konzept dagegen neben einem Mikrocontroller im Zentrum des Rechnersystems auf eine ausreichend unabhängige, mithin separate Hardwareinstanz für Überwachungsaufgaben, die außerdem klein und preisgünstig ausfallen soll.

[89] Silizium-Substrat, Halbleitergrundfläche
[90] Damit sind ECUs für typische Fail-Safe-Anwendungen oder auch mit Fail-Operational-Verhalten und degradierter Funktion und/oder Sicherheitsintegrität für Notläufe gemeint.

Während bei EGAS parallel zu den eigentlichen Funktionen auf Ebene 1 auf Ebene 2 vergleichbare Funktionen und auf Ebene 3 entsprechende Rechenaufgaben berechnet und die richtigen Ergebnisse in der externen Instanz überwacht werden, um die Hardwaresicherheitsintegrität des Rechnersystems zu kontrollieren, wird durch das neue Konzept zeitlich unmittelbar jedes einzelne Funktionsergebnis überwacht, um somit direkt die Hardwaresicherheitsintegrität der Ausgabewerte sicherzustellen.
Wesentlicher Unterschied ist also, dass direkt die Integrität der Ausgabe sichergestellt wird, unabhängig davon, welche Ressourcen des Rechnersystems wie RAM, ROM, CPU, Register, etc. dafür eingesetzt wurden. Die Rechenaufgaben und Überwachungen auf Ebene 3 im EGAS-Konzept überwachen streng genommen lediglich die Teile des RAM, ROM und anderer Ressourcen, die für die parallelen Funktionsrechnungen auf Ebene 2 zum Einsatz kommen. Je mehr den eigentlichen Funktionen des Rechnersystems nachempfundene Rechenaufgaben gestellt und kontrolliert werden, desto besser ist zumindest die Aussage über die Integrität der CPU. Auch im neuen Konzept kann eine allgemeinere Aussage zur Integrität der CPU abgeleitet werden, um beispielsweise Nachweise zur Sicherheitsintegrität gegen SPFs für Nebenaufgaben wie Gradientenberechnung oder Gateway-Funktionen erbringen zu können. Vorteilhaft an dem Konzept ist dabei, dass neben der Linearfunktion f(e) auch eine entgegen gerichtete Funktion g'(a) mit unterschiedlicher Datenbasis berechnet und kontrolliert wird und damit ein deutlich größeres Spektrum aller möglichen Operationen[91] der CPU abgedeckt wird. Der DC eines oft nur rudimentär implementierten CPU- und Registertests liegt erfahrungsgemäß weit unter 60% und erreicht damit nicht einmal die Stufe "niedrig" bei den in den Normen genannten SMs. Trotzdem kann in den entsprechenden FMEDAs ein bestimmter Prozentsatz DC zum Ansatz gebracht werden. Für die beiden oben genannten Funktionen als CPU- und Registertest können allgemein vielleicht 10% bis 30% Aufdeckung gefährlicher Fehler angesetzt werden, je nach sonstigen Aufgaben der CPU und entsprechenden, weiteren Sicherheitszielen.
Zur Taktüberwachung bei EGAS ist ein externer Fenster-Watchdog vorgesehen, der allerdings, je nach zeitlichen Anforderungen und Bedingungen, durch die ohnehin vorgesehene externe Hardwareinstanz zur Überwachung mit übernommen werden könnte. Voraussetzung für die richtige Wirkung ist dabei jedoch, dass die vom Mikrocontroller ausgehenden Meldesignale (Trigger) an den Fluss des Programms zur Ausführung der eigentlichen Funktionen und nicht etwa nur an die Rechenaufgaben zur Überwachung geknüpft sind und dabei ein sinnvolles, zeitliches Überwachungsfenster treffen. Im neuen Sicherheitskonzept sind diese Bedingungen durch die direkte Überwachung aller zyklischen Funkti-

[91] zumindest die aller 4 Grundrechenarten unter Einsatz aller ALU- und Allzweck-Register der CPU

onswerte in Größe a sozusagen „in time“ gewährleistet. Ein nicht rechtzeitig eintreffender Vergleichswert führt sofort zum Ausbleiben der qualifizierenden Botschaft bzw. zum Abschaltvorgang.

Bezüglich Spannungsversorgung wird für das Konzept EGAS keine Überwachungsmaßnahme genannt. Undefinierte Überspannungen des einfach vorhandenen Spannungsreglers könnten als gemeinsame Ursache (en: common cause, CC) sowohl den Mikrocontroller wie auch die externe Überwachungshardware kompromittieren und letztlich gefährliche Ausgaben zulassen. Abhilfe könnte ein zweiter Spannungsregler im System oder eine vom Mikrocontroller unabhängige Überwachung, vor allem gegen Überspannung, bringen, die allerdings selbst gegen Überspannung stabil ausgelegt sein müsste. Im neuen Sicherheitskonzept sind zweiter Spannungsregler und Überwachungseinrichtung in mindestens einem der ohnehin vorhandenen Sensorbausteine vorgesehen und im vorgestellten Hall-Sensor-IC MLX90363 bereits integriert.

Um die Sicherheitsintegrität der Rechner-HW auch in Fällen der Anwendung unter Wegfall der Vergleichsinstanz sicherzustellen (Notlauf bei ASIL B(D), ASIL B ohne Nutzung des ASIL-Qualifiers), muss ähnlich wie für den Sensorbaustein vorgegangen werden (siehe vorheriger Abschnitt). Zur Verfügung stehen die zur Absicherung eines Rechnersystems herkömmlichen Mittel und Mechanismen, wie sie beispielsweise unter Abschnitt 4.2 genannt wurden.

### 8.2.3 HARDWARESICHERHEITSINTEGRITÄT DER VERGLEICHSEINRICHTUNG

Kern des neuen Konzepts ist die in den zweiten Sensorbaustein S2 integrierte Vergleichseinrichtung V, mit der die aus zwei Messungen resultierende funktionelle Diversität bis zum Ausgabewert asymmetrisch am Ort der zweiten Messung zusammengeführt und plausibilisiert wird. Durch diesen Sicherheitsmechanismus (AAV) kann die Korrektheit und vollständige HW-Sicherheitsintegrität von S1 und dem Rechnersystem MC unabhängig von diesen sichergestellt werden. Ein solcher Vergleich direkt in MC könnte durch einen einzigen Ausfall im Silizium dort bereits kompromittiert sein. Die über S1 von MC zum Vergleich in S2 angebotene Winkelgröße e' muss bei Übereinstimmung mit der von S2 korrekt entstanden oder genügend unwahrscheinlich erraten worden sein. Weder S1 noch MC kann richtige Vergleichswerte für e' an irgendeiner Stelle kopieren oder ablesen. Mithin müssen auch die in MC zwischendurch zur Ausgabe bereitgestellten Absolutwinkelwerte korrekt sein. Diese Aussage kann sogar für jeden erhobenen Messwert oder Absolutwinkelwert im Beispiel des LWS gelten. Sooft gemessen und ein Absolutwinkel berechnet wird, und dies kann mit dem vorgestellten Sensorbaustein MLX90363 gemäß Datenblatt pro Millisekunde einmal geschehen, kann die Richtigkeit der entspre-

chenden Ausgabe a durch V belegt werden. Diese Kontrollfrequenz sollte stets zu den Fahrzeugfunktionalitäten mit Lenkwinkel bis Stufe ASIL D und zu deren üblichen Fehlertoleranzzeitintervallen passen.
Voraussetzung für diese sicherheitstechnisch sehr starke Aussage des Vergleichsergebnisses ist natürlich ein korrekt arbeitender Vergleichs- und Abschaltmechanismus selbst.
Ein zufälliger Ausfall bzw. entsprechender Fehler in V ist jedoch zunächst noch nicht kritisch, weil er allein nicht das Potential zur Verletzung eines SZs hat. Erst ein weiterer Fehler im System, beispielsweise in S1 oder in MC kann zu falschen und damit gefährlichen (Winkel-)ausgaben führen. Es geht hier also ausschließlich um die Vermeidung von latenten Ausfällen in V und auch nur um diejenigen, die sich in Kombination mit anderen Ausfällen gefährlich auswirken könnten. Ein unbeabsichtigt ausgelöstes Abschaltsignal könnte zwar den Betrieb der eigentlichen Funktionalität beenden, wäre jedoch nicht als sicherheitskritisch zu werten. Erst eine fehlerbedingte, positive Kontrollbestätigung (Ausgabe des einen, speziellen ASIL-Qualifiers), korrekt durch CRC und Botschaftszähler abgesichert bei einem durch S1 oder MC gleichzeitig falsch ermittelten Ausgabewinkelwert kann das betrachtete Lenkwinkelsensormodul insgesamt gefährlich machen.
Die Wahrscheinlichkeit für speziell diesen Fall, dass ausgerechnet und genau die wenigen Transistoren auf dem Die vom Ausfall betroffen sind, die den Vergleich (siehe Pseudocode in Abschnitt 7.5) am Ende positiv passieren lassen, und der Defekt des Bausteins nicht bereits an anderer Stelle, z.B. durch die in Abschnitt 8.2.1 genannten Diagnosen in S2 auffallen (z. B. durch die integrierten RAM-, ROM- und CPU-Tests), wird dem Restrisiko zugerechnet und akzeptiert. Die Vergleichseinrichtung in S2 macht nur einen sehr kleinen Teil des Bausteins insgesamt aus. Ihre Hardwaresicherheitsintegrität im Verhältnis zum gesamten Baustein oder erst zum gesamten Item aus Sicht der ISO 26262 fällt bei der Berechnung der Hardwarearchitekturmetrik LFM nicht ins Gewicht und gibt quasi keinerlei Ausschlag darin.
Um ganz sicher zu gehen, wäre ein eingebauter Test der Vergleichs- und Abschalteinrichtung denkbar, für die der MC im Rechnersystem zum Systemstart probeweise einen bewusst falschen Vergleichswert für e' anbietet und an S2 überträgt. Am von S2 zurückgelieferten ASIL-Qualifier, der in diesem Fall den Default-Wert für Nichtübereinstimmung (en: mismatch) haben sollte, kann MC entscheiden, den Vergleich im Konzept weiter einzubeziehen oder eben für den anstehenden Fahrzyklus als defekt zu melden und infolge dessen zu ignorieren.
Auch ein ausschließlich in HW realisierter Vergleichs- und Abschaltmechanismus könnte sporadisch, z.B. beim Systemstart, geprüft werden. Hierzu würde dann die von V in S2

ausgehende Abschaltleitung an MC geführt, ihre Information zurückgelesen und auf den für den Fall der Abschaltung korrekten Inhalt hin geprüft werden. Konzeptionell ideal für das Abschaltsignal ist jedenfalls der spannungslose Ruhezustand (low) für alle Fälle, bei denen die Integrität nicht durch ein positiv übereinstimmendes Vergleichsergebnis sichergestellt werden kann.

Natürlich sind weitere, technische Lösungen zur Überprüfung des Vergleichsresultats und zur weiteren Stärkung des Konzepts denkbar. Ein in S2 und analog auch in S1 ohnehin vorhandener IP-Block "µC" bietet sich bei entsprechenden Ergänzungen der Firmware dazu an. Beispielsweise könnten die Umkehrfunktion e = u(g)(e') und/oder die Umkehrfunktion a = u(e') aus den gemessenen Werten e' berechnet und dem Vergleichsergebnis zur zusätzlichen Plausibilisierung beigefügt werden. Auch andere - einfache - Signaturen könnten ermittelt und dem Vergleichsergebnis als weitere gemeinsame Kennzeichen zur externen Überprüfung beigefügt werden. Alle solchen Möglichkeiten sollen aber im Rahmen dieser Arbeit nicht weiter betrachtet werden, um auf dem für ASIL D ausreichenden und praxisnahen Minimalkonzept beschränkt zu bleiben. Oft wird an die Konzepte verteilter Systeme im Automobil die Anforderung gestellt, dass ihre Module bei aller Einfachheit so autark wie möglich voneinander bleiben, um die Abstimmung bei den meist verteilten Entwicklungen innerhalb der Zuliefererkette zu vereinfachen und um die Möglichkeiten der Wiederverwendung bestehender Komponenten zu verbessern. Auch das Modul zur Lenkwinkelerfassung soll demnach für sich sicherheitsintegere Daten liefern. Die Einheiten der Aktorik sollen z.B. nach Möglichkeit keine Mechanismen mehr zur Absicherung der Sensorikmodule enthalten müssen. Aufwändige und über die Fahrzeugsysteme verteilte SMs (abgesehen von E2E-Absicherungen) werden grundsätzlich gern vermieden.

Ähnliche Überlegungen und Begründungen zur Integrität des Vergleichs gelten analog auch für die nachgeschaltete Fehlerreaktion bzw. die Abschalteinrichtung. Bei der digitalen Realisierung des Sicherheitsmechanismus mit seriell übertragener Botschaft geht es um die Integrität der Ende-zu-Ende-Absicherung. Auch hier sind die weitaus meisten Ausfälle (> 99%) sichere Ausfälle, weil nur ein einziger richtiger Weg zu einer korrekten CRC-Prüfsumme und einem korrekten Botschaftszähler führt, die am Ende des grauen Kanals beim Empfänger des Vergleichsergebnisses (ASIL-Qualifier) kontrolliert werden. Dem Konzept steht nicht entgegen, wenn diese Zusatzdaten zwischendurch auch schon von MC in seiner Gateway-Funktion hierfür geprüft werden. Beim LWS im Beispiel wird dies während der Initialisierung ohnehin geschehen. Hier werden nämlich zwecks erster Bestimmung eines Absolutwinkelwerts nach dem Noniusprinzip die mit Sicherheitsredundanz versehenen Messwerte aus beiden Sensorbausteinen ausgelesen.

Beim Sicherheitskonzept EGAS wird die eingesetzte, externe Hardwareinstanz, ohne die eine insgesamt höhere HW-Integrität nicht erreicht werden kann, manchmal „intelligenter Watchdog“ genannt. Die eigene Integrität dieses „Überwachungsrechners“ auf Ebene 3 wird selbst in keiner Weise kontrolliert. Allerdings hat diese Einrichtung ähnlich wie bei der AAV des neuen Konzepts nur triviale Aufgaben zu verrichten, sodass hier ebenfalls nicht mehr viel zu überwachen ist. Dennoch muss neben entsprechenden Vergleichen auch eine bestimmte Reihenfolge der Überwachungen und ihre richtigen Ergebnisse verwaltet werden, weshalb die ganze Einrichtung nicht diskret (ausfallsicher) verdrahtet oder gar in Analogtechnik realisiert werden kann. Der Abschaltmechanismus hingegen ist wiederum rein hardwaretechnisch mittels elektrischer Leitungen vorgesehen. Es gibt im EGAS-Konzept keine Möglichkeit der flexibleren Abschaltung oder Fehlerkommunikation per digitalem Signal und SW. Stattdessen sind für den Fehlerfall ausschließlich diese Leitungen vorgesehen, die die Aktorik entsprechend deaktivieren können. Dies stellt im Hinblick auf notwendige Notlaufkonzepte und/oder weitere, weniger kritische Funktionalitäten, die auf dieselbe Sensorik und gleiche Messgrößen angewiesen sind, einen großen Nachteil dar. Die entsprechenden Abschaltleitungen müssten separat an jeden Ort im Fahrzeug geführt werden, an dem gewisse Funktionalität unter Umständen degradiert bzw. abgeschaltet werden muss. Deshalb ist das neue Konzept an diesem Punkt flexibler und wegen seiner Realisierungsoptionen für zusätzliche SMs auch insgesamt sicherer.

## 8.3 Fremdeinflüsse und deren Beherrschung

Wie bereits angesprochen kann der zufallsbehaftete, physikalische Einfluss von außen zu permanenten oder auch nur transienten Ausfällen an Teilen der Betrachtungseinheit führen.

In Zusammenhang mit mechanischen, chemischen, thermischen, elektromagnetischen, elektrostatischen oder auch magnetischen Einwirkungen entstehen wegen Materialermüdung, Auflösung, Alterung, Zerstörung oder anderer Ursachen Fehler im Produkt, die mitunter gefährlich werden können, wenn sie nicht im Betrieb erkannt und beherrscht werden. Da das Wesentliche des neuen Sicherheitskonzepts eine funktionelle Diversität ist, die weite Teile des (Sub-)Systems überdeckt und dadurch einzelne Ausfälle im Betrieb auffallen müssen, verbleiben zur Betrachtung vor allem zufällig entstehende Fehler, die durch die AAV nicht erkannt werden können. Hierzu zählen einerseits Fehler an Bauteilen außerhalb der diversitären Bereiche und andererseits Fehler, die entweder auf mehreren, gleichzeitigen Ausfällen basieren oder aber auf gar keinem Ausfall, keiner Veränderung des Systems basieren, sondern auf anderen, äußeren Einflüssen beruhen.

Die ersteren Fehler können sich im Beispiel Lenkwinkelsensor nur auf die Antriebsmechanik beziehen und werden im nächsten Abschnitt 8.4 behandelt. Die andere Gruppe von Fehlern, sofern sie mit einer Veränderung des sicherheitsgerichteten Produkts zu tun hat, ist äußerst unwahrscheinlich. Solche Fehler kommen nur dann zustande, wenn die gemeinsame Ursache zufällig in beiden diversitären Pfaden solche Ausfälle bewirken würde, die trotz funktioneller und Datenverschiedenheit wieder zu einem einheitlichen Ergebnis im Vergleich der AAV führen. Übrig bleiben nun nur noch die Fehler, die nicht auf Veränderungen im Produkt basieren und durch ihre äußere Wirkung trotzdem zu einem positiven, aber kausal falschen Vergleichsergebnis führen.

Für das spezielle Beispiel eines magnetischen Lenkwinkelsensormoduls stellt sich damit vor allem die Frage, in wie fern ein fremdes magnetisches Feld beide im Konzept vorgesehenen Messstellen gleichzeitig und derart beeinflussen und die eingesetzten Magnetgeber überlagern kann, sodass letztlich ein falscher Absolutwinkel korrekt berechnet, plausibilisiert und ausgegeben wird.

Übliche, in Messräder eingebrachte Magnetgebersysteme bestehen aus Neodym-Verbundmaterial mit einer für hohen Störabstand möglichst hohen magnetischen Flussdichte. Gemäß Datenblatt des vorgestellten Messbausteins MLX90363 erwartet das IC eine ihn durchziehende magnetische Flussdichte von 20 bis 70 mT (Millitesla). Zu niedrige und auch zu hohe Flussdichten werden erkannt und führen zur Einstellung der Winkelmessvorgänge. Das zur Winkelmessung notwendige Magnetfeld wird z.B. durch zwei kunststoffgebundene Magnetkörper aufgespannt, die sich in einem Messrad befinden und sich mit um dessen Achse drehen.

Das durch solche Permanentmagnetkörper gebildete Magnetgebersystem, jeweils in möglichst unmittelbarer Umgebung von Mess- und Kontrollsensor-IC positioniert, muss daher bereits in sich eine Stärke haben, die durch übliche Fremdmagnetfelder in der Nähe der Lenksäule hinter dem Lenkrad in aller Regel nicht zu verfälschten oder nur zu geringfügig verfälschten und damit noch sicheren Messungen führt. Als Gefahr in Frage kommen können daher nur von außen an das Sensormodul manuell – zufällig, demonstrativ oder eher vorsätzlich – angebrachte Magnetsysteme. Ihre magnetische Wirkung (auf eisenhaltige und magnetische Körper) nimmt mit dem Abstand zum Magneten sehr stark ab. Ihr Magnetfeld ist abhängig von Stärke, Form und Größe des Magneten und des Gegenkörpers. Damit sich durch das in diesem Fall als Abstandshalter fungierende Kunststoffgehäuse hindurch überhaupt eine die Messung verfälschende Wirkung zeigt, werden Magnete mit sehr großer magnetischer Flussdichte (z.B. Monstermagnete im Bereich 1 Tesla und mehr) benötigt. Zudem dürfte die maximal zulässige Messflussdichte durch den Einfluss

eines Magneten von außen auch in keinem der beiden Messsysteme überschritten werden. Es ist daher sehr unwahrscheinlich, dass ein nicht erst im laufenden Betrieb angelegter, einzelner Fremdmagnet auf beide Messräder einen sicherheitsverletzenden Einfluss ausübt. Völlig ausgeschlossen ist dies aber nicht. Eine an beide Messstellen symmetrisch angelegte und die Messmagnetsysteme deutlich überlagernde Feldstärke mit einem geeigneten Verlauf der Feldlinien und vom Beginn der Messungen an könnte vom Start weg und konstant einen Messwert bewirken, der tatsächlich nicht der realen Winkelstellung des Lenkrades entspricht. Eine entsprechende Konstellation kann aber durch geometrische Maßnahmen unterbunden werden, wie später noch erläutert wird.

Aller Unwahrscheinlichkeit zum Trotz müsste ein den Messwert im Betrieb empfindlich treffendes Störmagnetfeld von außen außerdem Einfluss auf beide Messstellen gleichzeitig haben, sodass der Störeinfluss auch bei der Kontrolle an zweiter, diversitärer Messstelle unentdeckt bliebe. Der Einfluss eines einzelnen Fremdmagneten im laufenden Messbetrieb mit zwei sich gleichsinnig drehenden und miteinander plausibilisierten Magnetsystemen kann also nicht zu gefährlichen Resultaten führen, zumal auch plötzliche Winkelsprünge im System als Fehler überwacht und aufgedeckt werden.

Theoretisch noch nicht ganz ausgeschlossen werden können dagegen gefährliche Verfälschungen, die durch mehrere Fremdmagnete während der Initialisierung des LWS bewirkt würden. Abgesehen davon, dass aber der bei der Initialisierung ermittelte Absolutlenkwinkel für SZs mit ASIL D irrelevant ist (relevant dafür ist nur der Winkeländerungswunsch des Fahrers), würde die initial falsch ermittelte Absolutwinkelstellung nach spätestens einer drittel Lenkradrunde, dem Übersetzungsverhältnis nach etwa einer Runde des Messrades, durch die ständigen Vergleiche auffallen. Die Drehung der Messmagnetfelder im anlaufenden Betrieb kann nicht fremd so stark überlagert sein, dass insgesamt stets gültige Messungen mit unter 70 mT zustande kommen.

Zur weiteren Absicherung des Messsystems gegen Magnetfeldüberlagerungen kommen weitere konstruktive Maßnahmen in Betracht. Neben einem einen Mindestabstand sichernden Gehäuse eignet sich eine Anordnung der Magnetzahnräder, bei der sich diese um die ferromagnetische Lenksäule samt Antriebsrad gegenüberstehen. Zum einen ergibt sich dadurch ein größtmöglicher Abstand der Magnetsysteme zueinander. Zum anderen kann dadurch eine magnetische Abschirmung und Unabhängigkeit der beiden Messmagnetsysteme voneinander erreicht werden. Eine weitere, ferromagnetische Abschirmung des gesamten LWS nach außen hin ist als Lösung an dieser Stelle unverhältnismäßig aufwändig und damit wohl unwirtschaftlich.

## 8.4 Mechanische und weitere sicherheitstechnische Aspekte

Mechanische Veränderungen einer mechatronischen Komponente wie z.B. Zahnradbruch, Magnetkörperbruch, Magnetkörperzersetzung oder Loslösung von Bauteilen oder -elementen der Sensorik unterliegen im Bereich „other technology“ zwar nicht mehr direkt der Betrachtung der Norm ISO26262 für Fahrzeugelektrik und -elektronik. Trotzdem sollten diese Fehlermöglichkeiten für ein hohes Maß an Funktionssicherheit für mechatronische Produkte, z.B. auch in jeweiligen TSKs, betrachtet werden. Hierzu dienen vor allem FMEAs für System und Konstruktion, beispielsweise nach VDA-Standard (Band 4, Kapitel 3). Als weitere Analysen für diesen Bereich sind Toleranzrechnungen und Festigkeitsrechnungen üblich und vorgesehen. Davon abgeleitete, mechanische oder mechatronische Maßnahmen sind in aller Regel Überdimensionierung und später ein intensiver Umgebungstest mit Temperatur-, Stör-, Stress- und Belastungstests samt Dauerläufen.

Mechanische Veränderungen, die nicht einseitig den einen oder den anderen Pfad der diversitären Konzeptstruktur betreffen und sich damit direkt gefährlich auswirken können, sind im mechanischen, nichtredundanten Eingangsbereich des Sensormoduls zu suchen. Bauteile in diesem Bereich sind für das LWS-Modul die Lenksäule, die Mitnahme des Sensorantriebsrads und das Antriebsrad mit seiner Verzahnung selbst. Jedes dieser Teile kann beispielsweise durch Auflösung zu dem kritischen Fehler führen, dass weder Mess- noch Kontrollrad angetrieben werden. Fortan bliebe das Modul mit der korrekt scheinenden Ausgabe eines Lenkwinkels stehen, obwohl eine zwischenzeitliche Drehung des Lenkrades die Information einer Lenkwinkeländerung ins Fahrzeugsystem hinein hätte bewirken müssen.

Für konstruktive Gegenmaßnahmen gilt generell das Prinzip Unterlastung. Dies bedeutet eine entsprechend robuste Ausführung der (im LWS-Beispiel drei) betroffenen Bauteile gegen äußere mechanische Kräfte und alle anderen denkbaren, physikalischen Einflüsse. Bedeutende, intern wirkende Kräfte im System sind beim Antrieb der möglichst leichtgängigen und lautlosen Messräder beim LWS nicht zu erwarten.

Die Verbindung bzw. Mitnahme zwischen Lenkachse und Antriebsrad sollte aber nicht aus einem einzelnen Zapfen oder Mitnehmer bestehen, sondern könnte aus einem Bauteil mit mehreren symmetrisch angeordneten Verbindungsstellen bestehen. Dies hätte neben dem Effekt der Redundanz den Vorteil, dass das Antriebsrad nicht einseitig exzentrisch angetrieben, sondern möglichst zentrisch um die Lenkachse geführt wird. Damit kann sogar eine bessere Messgenauigkeit der Komponente erreicht werden, die in der Regel wieder in Zusammenhang mit SZs steht.

In einem sicherheitsbezogenen LWS wird es bei den SZs stets um die Ausgabe eines Lenkwinkels mit einer bestimmten, sicherheitstechnisch erforderlichen Genauigkeit gehen. Die erreichbare Genauigkeit wird in erster Linie von der Mechanik und ihrer Präzision abhängen. Durch die Übersetzung von etwa 1:3 des Lenk- oder Antriebsrades auf die Messräder wird in einem sozusagen vergrößerten Maßstab und dadurch wieder genauer gemessen. Beispielsweise wirkt sich wegen der Vergrößerung des Maßstabs die Genauigkeit des Magnetschaltkreises von angenommen 1,5° als Ungenauigkeit des Lenkradwinkels von 0,5° aus. Die Ungenauigkeit durch die Mikroelektronik und der darin implementierten Rechenalgorithmen spielt eine eher untergeordnete Rolle. Allerdings hat die Mikroelektronik mit ihrer SW die Aufgabe, neben den eigenen Fehlern auch Unplausibilitäten der Mechanik und der Magnettechnologie zu erkennen. Der sichere Zustand (im Fehlerfall) des Lenkwinkelsensormoduls ist eine Abschaltung oder Degradation der zugehörigen Fahrzeugfunktion, softwaretechnisch z.B. in Form einer Ungültigkeitsbotschaft. Die Information des Lenkwinkelsensors an die Anwendung im Fahrzeugsystem (z.B. ESP), dass der gerade ermittelte Wert des Winkels ungültig ist, muss innerhalb einer bestimmten, kritischen Zeit, der sogenannten zulässigen Fehlerreaktionszeit ausgegeben werden. Gründe für die Ausgabe dieser Ungültigkeitsinformation zur Abschaltung des Systems können sein, dass der Winkel unplausibel weit vom erwarteten Wert abweicht, er nicht in der mit dem SZ spezifizierten Toleranz liegt oder dass schlicht eine der untergeordneten Diagnosemechanismen einen Fehler erkennt. Als weiteren sicheren Zustand muss immer auch das Ausbleiben der Botschaft mit dem Lenkwinkel an das Fahrzeugsystem definiert werden. Die abhängigen Anwendungen müssen also den regelmäßigen Empfang von gültigen Lenkwinkelwerten innerhalb der für sie definierten, zulässigen Fehlerreaktionszeitintervalle (als Teil des definierten FTTIs) überwachen und gegebenenfalls abschalten. Der Lenkwinkelsensor könnte z.B. wegen eines jederzeit möglichen Stromausfalls außer Betrieb gegangen sein, was sich dann im gesamten System nicht kritisch auswirken darf.

Prinzipiell wirken sich eine höhere Integration von Schaltungsfunktionen und die dadurch ermöglichte Reduzierung von Bauteilen und -elementen günstig auf die Kosten eines Moduls, aber vor allem auch auf seine Funktionssicherheit aus. Je weniger Bauteile verwendet werden, desto einfacher durchschaubar und analysierbar ist das Konzept. Es müssen die Ausfälle von weniger Bauteilen betrachtet werden und die Anzahl zu betrachtender (Sicherheits-)Risiken reduziert sich. Auch von daher profitiert das in der vorliegenden Arbeit beschriebene Konzept zu Gunsten der Sicherheit gegenüber EGAS. Für entsprechende Realisierungen werden weniger Bausteine benötigt und die ganze Entwicklung gestaltet sich dadurch noch einfacher. Außerdem kann man mit bereits gebräuchlichen

elektronischen Komponenten und ICs auskommen ohne erst neue entwickeln zu müssen. Jede Neuentwicklung von integrierten oder kundenspezifischen Schaltkreisen wirft nämlich wieder neue Sicherheitsrisiken auf. Es bedarf also einer gründlichen Abwägung hierzu, wenn bei der Konzeption eines sicherheitsgerichteten Systems noch höher integriert werden soll, beispielsweise wie bei der Planung eines Hall-Sensorschaltkreises mit zusätzlich integrierter CAN-Schnittstelle.

# 9 ZUSAMMENFASSUNG UND AUSBLICK

## 9.1 BEITRÄGE UND ERGEBNISSE

In der Automobilbranche haben elektronische Komponenten nicht nur seit Jahrzehnten Einzug gehalten, sondern sind mittlerweile zum dominierenden Faktor für die meisten Fahrzeugfunktionen geworden. Auch die Funktionssicherheit für diese Komponenten ist nicht erst seit Erscheinen der entsprechenden Norm ISO 26262 für Personenkraftwagen bis 3,5 t im Jahr 2011 erfunden worden, sondern begleitete die Entwicklungen elektronischer Produkte für das Automobil seit vielen Jahrzehnten. Wenn auch der systematische Ansatz zur Entwicklung sicherheitsbezogener Funktionalitäten und konkrete Anforderungen dafür erstmalig mit dieser sektorspezifischen Norm festgeschrieben wurden, hatten sich bereits etliche Methoden, Verfahren und Arbeitsweisen zur Verbesserung der systematischen Integrität der Produkte etablieren und verfeinern können.

Der andere Bereich funktionaler Sicherheit, nämlich der der HW-Integrität gegen zufällig zustande kommende Sicherheitsausfälle wurde schon von Anbeginn gründlich betrachtet, weil sich Funktionssicherheit für Großserien von Personenkraftwagen nicht unbedingt für jeden Preis vertreiben lässt. Dieser Umstand führte seit Anfang der 1990er Jahre zur Entwicklung, Pflege und Verfeinerung des sogenannten EGAS-Sicherheitskonzepts. Dieses auf nur einem einzigen, nichtredundanten Rechnersystem beruhende Konzept gilt in der Branche auch heute noch als Basis und De-Facto-Standard für höchste Funktionssicherheit. Es ist in den letzten Jahren allerdings etwas unter den Verdacht geraten, nicht wirklich immer alle SZs und Sicherheitsanforderungen bis zur höchsten Integritätsstufe ASIL D abdecken zu können.

Hauptaufgabe dieser Arbeit war es, in diesem Umfeld und auf Basis eigener Erfindungen ein neues technisches Sicherheitskonzept auszugestalten (siehe Kapitel 6), dieses zum Einsatz zur Lenkwinkelerfassung zu bringen (siehe Kapitel 7) und in Gegenüberstellung zum bekannten EGAS-Konzept sicherheitstechnisch gründlich zu bewerten (siehe Kapitel 8). Das neue Konzept sollte ebenfalls mit einem einzigen Rechnersystem auskommen, jedoch die maximal mögliche Hardwaresicherheitsintegrität des bekannten EGAS-Konzepts übertreffen und Anwendungen im Bereich ASIL D ermöglichen. Weiteres Ziel war es, im Sinne der Sicherheit den Grad der Komplexität und die Anzahl der notwendigen Bauelemente zu minimieren. Nach Möglichkeit sollten durch das Konzept an sich auch systematische Fehler beherrscht werden können. Ein entsprechendes Produkt wird dadurch einfacher und sicherer und lässt sich in den verschiedenen Integrationsphasen der Entwicklung leichter gegen diesen Fehlertyp verifizieren.

Das so entstandene Konzept erfüllt die an es gestellten Anforderungen. Zur Erreichung dieses Ziels kommt eine funktionelle Diversität zum Einsatz, die sich über weite Teile der Signalpfade erstreckt. Kern des neuartigen Sicherheitskonzepts ist dann ein speziell angeordneter Vergleich zur Plausibilisierung der so aufgespannten Redundanz in der Betrachtungseinheit. Der Vergleich findet nämlich unabhängig vom Rechnersystem in einer asymmetrisch angeordneten Vergleichseinrichtung (AAV), integriert in einem zweiten Sensorbaustein statt. Er wird deshalb „asymmetrisch angeordnet“ bezeichnet, weil er auf einem vom Rechnersystem antivalent voraus und in entgegengesetzter Richtung zum eigentlichen Ausgabewert berechneten Vergleichswert beruht und eben nicht nach symmetrischer Zusammenführung im Mikrocontroller des Rechnersystem angeordnet ist.
Ob und in wie fern das entstandene, neue Konzept praktikabel ist und hinsichtlich der erreichbaren Sicherheitsintegrität auch dem wissenschaftlichen Blick standhält, konnte am Beispiel eines Lenkwinkelsensormoduls mit Magnettechnik aufgezeigt werden.
Die folgenden beiden Abschnitte fassen die Ergebnisse und sicherheitstechnischen Bewertungen in dieser Arbeit jeweils hinsichtlich der Hardwaresicherheitsintegrität und der systematische Sicherheitsintegrität des neuen Konzepts zusammen.

### 9.1.1 Asymmetrisch angeordneter Vergleich gegen zufällige Fehler

In diesem Abschnitt werden das neue Sicherheitskonzept und das Ergebnis der Untersuchungen hinsichtlich zufälliger Fehler in der HW zusammengefasst. Das zugehörige Fehlermodell für die Elektronikkomponenten im Ganzen ist durch Tabelle 8-3 und das für einen Sensor mit integrierter AAV im Detail durch Tabelle 8-4 definiert.
Das ganze Konzept besteht hardwaretechnisch im Wesentlichen aus nur drei mikroelektronischen Bausteinen: Einem ersten Sensorbaustein S1, einem Mikrocontroller MC und einem zweiten Sensorbaustein S2, in den auch die AAV mit dem entscheidenden Vergleich integriert ist. Daher wurde systematisch analysiert, ob die verschieden möglichen Ausfälle zur Laufzeit dieser drei Bausteine sicherheitsrelevant sind und falls ja, ob das Konzept die daraus resultierenden Fehler zu beherrschen vermag, sodass weder Einzelpunktfehler (SPF) noch latente Fehler (LF) unentdeckt bleiben. Funktionelle Diversität und die Unabhängigkeit des Vergleichs von der Funktionshardware sind die tragenden Säulen des Konzepts, die dafür sorgen, dass zur Beherrschung von Ausfällen im Funktionskanal in S1 und MC mit Potential zur Verletzung eines SZs mehr als 99% (SPF Metrik) angenommen werden darf. LFs dagegen, die in der vorgestellten Sicherheitsarchitektur des Konzepts nur in der Vergleichs- und Abschalteinrichtung in S2 auftreten könnten, können unter anderem durch die in die Sensorbausteine integrierten SMs beherrscht werden. Im Markt existierende Bausteine bieten dabei bereits Qualitäten und eine Abdeckung

solcher Fehlerbeherrschungsmechanismen an, die die Möglichkeit einer Latentfehlermetrik (LFM) von über 90% realistisch erscheinen lassen und im Einzelfall auch nachgewiesen werden konnten. Hinzu kommt, dass sich speziell ein kritischer Ausfall der AAV, des Vergleichs in S2, als sehr unwahrscheinlich herausgestellt hat. Die Gründe hierfür waren zum einen in dem prozentual sehr geringen, physikalischen Ausmaß der AAV innerhalb S2 und zum anderen in der sicheren Vorzugsrichtung bei einem Ausfall zu finden.

Obwohl die Anforderungen der ISO 26262 an Zielwerte für diese beiden Architekturmetriken nur im Querschnitt für die HW-Architektur einer Gesamtfunktionalität im Fahrzeug (Item) gelten, kann allein für ein konzeptbasiertes Teilsystem behauptet werden, dass die demonstrierten Werte trotz des nur singulären Rechnersystems für die Stufe ASIL D reichen. Die Stärke des Vergleichs als zentralem SM und vor allem seine Wirksamkeit in auch zeitlicher Redundanz für jedes Signal und jede Botschaft, die die betrachtete HW verlassen, macht das neue Konzept für SZs mit eng gesteckten Fehlertoleranzzeitintervallen brauchbar. Auch damit übertrifft es die Möglichkeiten des EGAS-Standards eindeutig.

Die Möglichkeit eines unabhängigen Abschaltpfads per abgesicherter, digitaler Botschaft (ASIL-Qualifier), die im EGAS-Konzept nicht, sondern dort nur als Deaktivierungsleitung zur kompletten Abschaltung vorgesehen ist, macht das Konzept recht flexibel. Bestehende Anwendungen im Fahrzeug, die zwar auf den Ausgabewert eines Sensormoduls mit dem Konzept und bis zur Stufe ASIL B angewiesen sind, aber nicht das Vergleichsergebnis benötigen, können ungehindert davon betrieben werden. Im Gegensatz zu EGAS können solche Anwendungen ganz unabhängig von der Abschaltung durch AAV weiter mit ausreichend validen Ausgangsdaten versorgt und unterstützt werden. Das Konzept erlaubt anderen, das Vergleichsergebnis einbeziehenden Anwendungen bis Stufe ASIL D unter Umständen sogar, Funktionalitäten in einem Notlauf unter entsprechend vermindertem ASIL fortzuführen. Diese Variabilität und Flexibilität kommt den wachsenden Anforderungen hinsichtlich automatisiertem Fahren und „Fail Operational“ sehr entgegen. Für vollautomatisches Fahren ohne mögliche Kontrollübernahme durch Menschen allerdings ist das Konzept hingegen – zumindest allein – nicht geeignet, weil auch im Fall eines einzelnen Ausfalls die für die SZs des Items definierten Sicherheitsintegritätsstufen nicht erhalten bleiben und nur noch vermindert gegeben sein sollten (ASIL D -> ASIL B).

### 9.1.2 Asymmetrisch angeordneter Vergleich gegen systematische Fehler

Gegenstand der Zusammenfassung in diesem Abschnitt ist der mögliche Beitrag des neuen Sicherheitskonzepts zur Vermeidung oder Erkennung von systematischen Fehlern, die bei

der Realisierung eines entsprechenden Systems eingebracht werden können. Das zugehörige Fehlermodell ist mit Tabelle 8-2 zugrunde gelegt. Diese Art Fehler sind in aller Regel durch die verschiedene Verifikation- und Validierungsschritte auf allen Ebenen der Entwicklung, besonders der Integration und der Fertigung eines Produkts und auf jeden Fall vor dem Einsatz im Fahrzeugbetrieb aufzudecken und zu beheben. Das neuartige Konzept vermag diese risikomindernden Vorgänge im Gegensatz zum EGAS-Konzept aber in zweierlei Hinsicht zu unterstützen.

Erstens können viele der systematischen Fehler, zum Beispiel die in überdurchschnittlich komplexer und an sich sicherheitsproblematischer SW-Technologie, durch erste Probeläufe schnell aufgespürt werden. Zu diesem Zweck hilft wieder die funktionell diversitär eingesetzte Redundanz, die sich im Konzept sowohl insgesamt über den größten Teil eines mechatronischen Produkts erstreckt, als auch für die Implementierung der SW im Rechnersystem (durch Umkehroperationen mit ungleichen Werten) schon im Kleinen besteht. Somit kann die korrekte Funktion des nur singulär vorhandenen SW-Systems schon in frühen Phasen mit Abschluss der SW-Prüfungen ausreichend verifiziert werden.

Zweitens stellte sich heraus, dass nur die AAV selbst systematische Fehler enthalten kann, die sich gefährlich auswirken und nicht schon durch die funktionelle Diversität im System sehr schnell auffallen werden. Die Vergleichs- (und Abschalt-) Einrichtung hat die Aufgabe, Werte in einem Analogspannungs- oder digitalen Wertebereich mit gewisser kleiner Toleranz zu vergleichen und nur im Falle der Übereinstimmung diese zu bestätigen bzw. eine Fehler- oder Abschaltreaktion zu unterbinden. Schon der vorgestellte Pseudocode bei einer programmatischen Realisierung verdeutlicht die Trivialität dieser Aufgabe. Die eigentliche Überwachung bedarf darin lediglich dreier Wertevergleiche bzw. Fallunterscheidungen. Die Verifikation der Einrichtung bis zum Start der Serienproduktion eines konzeptbasierten Produkts gegen alle Arten systematischer Fehler sollte damit sehr überschaubar bleiben. Vor diesem Hintergrund zur Verifikation ist das vorgestellte Sicherheitskonzept nicht nur dem bisherigen Sicherheitskonzept EGAS weit überlegen, weil dort viele einzelne Redundanzfunktionen und Überwachungsfunktionen verifiziert werden müssen. Das neue Konzept vermag in konkreten Produkten auf einfache Weise eine systematische Sicherheitsintegrität zu unterstützen, die ebenfalls den höchsten Sicherheitsanforderungen bei SZs auf Stufe ASIL D genügt.

## 9.2 Ausblick und zukünftige Arbeit

Zur beispielhaften Anwendung des vorgestellten Sicherheitskonzepts wurde in dieser Arbeit ein Lenkwinkelsensormodul (LWS) herangezogen. Die für das Konzept benötigte,

funktionelle Diversität mag für Sensormodule generell leichter herzustellen sein. Das Konzept sollte sich daher besonders gut auch für andere, hochgradig sicherheitsbezogene Sensormodule und sensorbasierte ECUs verwenden lassen, beispielsweise für Lenkraddrehmomentsensoren, Motorsteuerungen oder für Brems- und Gaspedalgebermodule. Da Prinzip und Konzept allgemeingültig sind, kommen sicherlich auch andere Industriezweige für Anwendungen in Frage. Hier sind wegen der einfachen und preisgünstigen Ein-Rechner-Architektur des Konzepts natürlich besonders Industrien mit Massenmärkten interessant, z.B. mit Schalt-, Steuer- und Regelgeräten für private Häuser und Heizungsanlagen. Aber auch Industrien mit generell hoher Anforderung an Funktionssicherheit, z.B. die Medizintechnik, stellen interessante Einsatzfelder dar.

Im Automobilsektor jedenfalls ist der Wunsch nach einfachen TSKs ohne vollredundante Rechnersysteme als Ersatz für das betagte und sicherheitstechnisch etwas schwächelnde EGAS-Konzept ungebrochen. Die aktuellen Trends der automatisierten Fahrerassistenz auf dem Weg zu vollautomatischem Fahren bedürfen gerade im Bereich der Sensorik Flexibilität, Notlaufeigenschaften und Fehlertoleranz auf höchstmöglichem Sicherheitsniveau, wie für Systeme mit dem neuen Konzept nebenbei sogar preisgünstig realisierbar scheint.

Bei der Anwendung im Einsatz LWS hat sich gezeigt, dass man für Produkte, die für kritischste Anwendungen zum Einsatz kommen sollen, zu Gunsten von Funktionssicherheit und deshalb zur strengen Vermeidung von Komplexität, mit hoher Priorität auf alle zusätzlichen und softwarebasierten Funktionen verzichten muss. Für einen konkreten LWS wird daher angeregt, unter Beibehaltung der Fehlertoleranz nur das Allernötigste für ausreichende Genauigkeit und die SZs mit dem höchsten ASIL vorzusehen. Für weniger sicherheitsgerichtete Anwendungen mit nur sekundärem Bedarf an Lenkwinkeldaten und ganz anderen Aufgaben könnte stattdessen eine separate ECU eingeplant werden, die alle zusätzlich benötigten Informationen und SW-Funktionen bereitstellt und auch die übrigen Anforderungen erfüllt.

Zur Verbesserung des soweit erarbeiteten Sicherheitskonzepts könnte man zum Beispiel an weitere Integrierung von Bauelementen denken. Weiteres Integrieren von Funktionen in die mikroelektronischen Bausteine im Konzept könnte am Ende das Konzept bezüglich Sicherheit weiter vereinfachen, nebenbei Herstellkosten sparen und vielleicht auch die Verifikation weiter erleichtern. Eine Idee hierzu ist zum Beispiel, die Schnittstelle des Bussystems für CAN komplett in die Sensorbausteine zu integrieren. Der in diesen IC-Bausteinen ohnehin schon vorhandene Digitalteil könnte sogar vielleicht auch schon die – relativ überschaubare – Aufgabe des ganzen Rechnersystems MC im Konzept überneh-

men. Dies bedeutete konkret, dass der erste Sensorbaustein S1 den fertigen Ausgabewert errechnet und in das CAN weiterleitet. Gegenüber dem zweiten Sensorbaustein S2 träte S1 als SPI-Master auf und würde dem als SPI-Slave verbundenen S2 einen vorausberechneten Wert zum Vergleich und zur Kontrolle übermitteln. Der Sensorbaustein S2 könnte bei Übereinstimmung mit dem eigenen Messwert eine bestätigende Botschaft über SPI via S1 oder seine eigene Systemschnittstelle direkt zur Aktorik senden. Als noch nicht gelöstes Problem bleibt für diesen Ansatz zunächst die Notwendigkeit der Kalibrierung zur initialen Bestimmung des Absolutwinkels über das Noniusprinzip, wenn wir im Beispiel des magnetischen LWS bleiben. Ein Rechnersystem mit Mikrocontroller und einem SW-System ist hier und auch, was Änderungswünsche angeht, auf jeden Fall flexibler als ein ASIC. Aber auch bei bestehen bleibendem MC könnte eine eigene Systembusintegration in S2 Sinn machen, um Common-Cause-Faktoren für die unabhängige Übertragung von Informationsdaten (z.B. Lenkwinkel) einerseits und Sicherheitsbestätigungsdaten (z.B. ASIL-Qualifier) andererseits zu reduzieren. Ein sicherheitstechnisch großer Nachteil bei allen Integrationsversuchen wird bleiben, dass dafür zunächst neue und damit unerprobte Bausteine oder ASICs entwickelt werden müssten.

Ein weiteres Projekt für die Zukunft des neuen Konzepts könnte eine Verfeinerung zur weiteren Flexibilisierung zur Anwendung mit Funktionsdegradationen oder für den Bereich Fehlertoleranz (Fail-Op) sein. Denkbar ist hier zum Beispiel eine Art Rollentausch für die beiden Sensorbausteine. Sofern ein Defekt zur Laufzeit eindeutig auf den ersten Sensorbaustein S1 zurückzuführen ist, könnte konzeptionell vorgesehen werden, dass der zweite Sensorbaustein S2, sozusagen nach „fliegendem Wechsel“, die Rolle der Messwertaufnahme von S1 übernehmen kann. Je nach Art und Ort eines zur Laufzeit diagnostizierten Ausfalls wären so bestimmte Fortsetzungen eines gesicherten Messbetriebs möglich.

Der ISO 26262 ist seit ihrer Veröffentlichung 2011 eine hohe Beachtung in der Funktionalen Sicherheit für den Automobilbereich zugekommen. In der Natur der Sache liegt, dass sie eher Vorgaben zur Methodik, also zur Verbesserung der systematischen Integrität machen kann als konkrete SMs und technische Sicherheitskonzepte wie das in dieser Arbeit vorgestellte vorzugeben. Trotzdem wären für zukünftige Versionen der Norm als jeweils gültiger Stand der Wissenschaft und Technik vielleicht Anhänge zum beispielhaften Vergleich verschiedener Prinzipien, Konzepte und HW-Sicherheitsarchitekturen sinnvoll. Insbesondere hinsichtlich automatischer oder gar autonomer Fahrfunktionen und dem Betrieb mit Fehlertoleranz liefert der gegenwärtige Stand der ISO26262 noch keine hinreichenden Konzept- oder Architekturvorgaben [78]. Ebenfalls sinnvoll in diesem Zusam-

menhang wäre die Ergänzung und Pflege eines Nachschlagewerks von Arten, Wirksamkeiten und Mitteln der Redundanz mit konkreteren Beispielen und Referenzen für den Systemarchitekten.

## REFERENZEN


[1] D. Grell, „Rad am Draht - Innovationslawine in der Autotechnik,“ Heise Verlag, 2013. [Online]. Available: http://www.heise.de/artikel-archiv/ct/2003/14/170. [Zugriff am 20 August 2010].

[2] H. Wallentowitz und K. H. Reif, Handbuch Kraftfahrzeugelektronik, Wiesbaden: Friedrich Vieweg & Sohn Verlag, 2006.

[3] R. Belschner, J. Freess und M. Mrossko, „Gesamtheitlicher Entwicklungsansatz für Entwurf, Dokumentation und Bewertung von E/E-Architekturen,“ VDI-Verlag , Düsseldorf, 2005.

[4] S. Kubica, W. Friess, T. Koelzow and W. Schröder-Preikschat, "Using signal-oriented feature trees for model-based automotive functions," *Proceedings of the 17th IASTED international conference on Modelling and simulation*, p. 459–464, 2006.

[5] Focus online, „Parkassistent - Volkswagen kann jetzt auch quer,“ 2010.

[6] C. Brünglinghaus, „Fahrerassistenzsysteme von Mercedes-Benz mit neuen Funktionen,“ 2009. [Online]. [Zugriff am 31 05 2014].

[7] L. Henle, U. Regensburger, B. Danner, E. Hentschel und C. Hämmerling, „Fahrerassistenzsysteme,“ *ATZ extra*, Bde. %1 von %2Die Neue E-Klasse von Mercedes Benz, Nr. 01, 2009.

[8] R. Isermann, K. Schmitt und R. Mannale, „Collision Avoidance PRORETA: Situation Analysis and Intervention Control,“ in s *IFAC-Symposium Advances in Automotive Controll AAC*, München, Germany, 2010.

[9] M. Ardelt, P. Waldmann, N. Kämpchen und F. Homm, „Strategic Decission-Making Process in Advanced Driver Assistance Systems,“ in s *IFAC-Symposium Advances in Automotive Control AAC*, München, Germany, 2010.

[10] M. Gräbner, „Brain Computer, Forschungsprojekte auf der CeBIT,“ *c't*, Nr. 38, 06 2010.

[11] E. Sax, Automatisiertes Testen eingebetteter Systeme in der Automobilindustrie, Carl Hanser, 2008.

[12] Robert Bosch GmbH, Sicherheits- und Komfortsysteme, R. B. GmbH, Hrsg., Vieweg+Teubner, 2004.

[13] M. Hillenbrand, Funktionale Sicherheit nach ISO 26262 in der Konzeptphase der Entwicklung von Elektrik / Elektronik Architekturen von Fahrzeugen, Karlsruhe:

Karlsruher Institut für Technologie (KIT), 2012.

[14] C. Ebert und D. Lederer, „Dem Kostendruck begegnen - Effizienz nachhaltig steigern.," *Automobil Elektronik,* p. 46–48, 10 2007.

[15] Süddeutsche Zeitung, „10.000 Einzelteile in einem Auto - viel Potenzial für Fehler," Süddeutsche Zeitung, 3 März 2010. [Online]. Available: http://www.sueddeutsche.de/auto/rueckrufaktionen-pfusch-ab-werk-1.16544-2. [Zugriff am 11 Januar 2015].

[16] V. Gebhardt, G. M. Rieger, J. Mottok und C. Gießelbach, Funktionale Sicherheit nach ISO 26262, Heidelberg: dpunkt Verlag, 2013.

[17] P. Löw, R. Papst und E. Petry, Funktionale Sicherheit in der Praxis: Anwendung von DIN EN 61508 und ISO/DIS 26262 bei der Entwicklung von Serienprodukten, dpunkt Verlag, 2010.

[18] J. Bösrcsök, Funktionale Sicherheit. Grundzüge sicherheitstechnischer Systeme, 1. Auflage Hrsg., Hüthig, 2006.

[19] CENELEC EN 61508, „EN 61508," Brüssel, 2010.

[20] ISO26262, "ISO 26262. Roadvehicles- Functional Safety, Part 1 - 9," Genf, 2011.

[21] J. Horstkötter, P. Metz und A. Ntima, „Funktionale Sicherheit und ISO 26262 - Entmystifiziert," F+S Fleckner und Simon Informationstechnik GmbH, 2010.

[22] H. Huppertz, „E-Gas (Electronic Accelerator Pedal)," 2001-2011. [Online]. Available: http://www.kfz-tech.de/EGas.htm. [Zugriff am 30 05 2014].

[23] A. Meyna, *Beitrag zur Entwicklung einer allgemeinen probabilistischen Sicherheitstheorie,* Gesamthochschule Wuppertal, 1980.

[24] E. Kramer, Passive Sicherheit von Kraftfahrzeugen, Biomechanik - Simulation - Sicherheit im Entwicklungsprozess, 1. Auflage Hrsg., Vieweg Verlagsgesellschaft, 2006.

[25] ISO, *ISO 25119 Tractors and machinery for agriculture and forestry -- Safety-related parts of control systems,* 2010.

[26] ISO26262-10, "Road vehicles - Functional Safety - Part 10: Guideline on ISO 26262," Genf, 2012.

[27] S. Kilimann, „ESP - elektronisches Stabilitätsprogramm. Mit dem Elchtest kam der Erfolg," 03 2010. [Online]. Available: http://www.auto-motor-und-sport.de. [Zugriff am 16 05 2012].

[28] ISO8402, „ISO 8402 Quality management and quality assurance – Vocabulary,"

1994.

[29] A. Birolini, Zuverlässigkeit von Geräten und Systemen, 1. Aufl. Hrsg., Berlin: Springer Verlag, 1997.

[30] A. Birolini, Reliability engineering. Theory and practice, Springer, 2004.

[31] F. Jondral und A. Wiesler, Grundlagen der Wahrscheinlichkeitsrechnung undstochastischer Prozesse für Ingeniere, Stuttgart: B. G. Teubner, 2000.

[32] C. Ronniger, Zuverlässigkeitsanalysen mit Weibull, 11. Auflage Hrsg., http://www.weilbull.de: Selbstverlag, 2010.

[33] Siemens AG, *Failure rates of components,* 1994.

[34] IEC, *IEC 62380 - Reliability Data Handbook,* 2004.

[35] IEC, *IEC 61709 Electric components. Reliability. Reference conditions for failure rates and stress models for conversion,* 2011.

[36] U. D. o. Defense, *Electronic Reliability Design Handbook,* 1998.

[37] W. A. Halang und R. Konakovsky, *Sicherheitsgerichtete Echtzeitsysteme,* Bd. I und II, München: Oldenbourg Industrieverlag, 2004.

[38] VDA Verband der Automobilindustrie e.V., Sicherung der Qualität vor Serieneinsatz - Produkt- und Prozess FMEA, 2. Auflage Hrsg., 2006.

[39] IEC International Electrotechnical Commission, *IEC 61025,* Genf, Schweiz, 1990.

[40] M. Müller, K. Hörmann, L. Dittmann und J. Zimmer, Automotive SPICE in der Praxis, Heidelberg: dpunkt Verlag, 2007.

[41] R. Kneuper, CMMI. Verbesserung von Softwareprozessen mit Capability Maturity Model Integration, Heidelberg: dpunkt Verlag, 2007.

[42] K. Echtle, Fehlertoleranzverfahren, Springer-Verlag GmbH, 1998.

[43] S. Herrmann, D. Dürholz und R. Stärk, Safety Essentials. ISO 26262 auf einen Blick - kompakt vermittelt, Kornwestheim: Kugler Maag Cie GmbH, 2014.

[44] ISO, *ISO15288 V-Modell. Systementwicklung – Der Lebenszyklus und seine Prozesse,* 2008.

[45] H.-L. Ross, Funktionale Sicherheit im Automobil. ISO 26262, Systemengineering auf Basis eines Sicherheitslebenszyklus und bewährten Qualitätsmanagementsystemen, München, Wien: Carl Hanser Verlag, 2014.

[46] H. Braun, „Wir sind auf dem Weg. Die Erforschung des autonomen Fahrens," *c't,* Nr. 9, pp. 136-139, 7 4 2014.

[47] D. Grell, „by-wire - doch ganz anders als im Airbus. Innovationslawine in der Autotechnik,“ *c't,* 03 2007.

[48] J. Schaffner, „Gefahrenanalyse und Sicherheitskonzept nach ISO 26262 für Fahrerassistenzsysteme,“ *ATZ elektronik,* pp. 34-39, Januar 2011.

[49] C. Rupp, Requirements-Engineering und -Management, Hanser Verlag, 2004.

[50] ISO, *ISO 15504 - Information Technology - Process Assessment,* 2004.

[51] Mira Ltd., „MISRA-C. Guidelines for the use of the C language in critical systems,“ MIRA Ltd., 2004.

[52] J.-C. Laprie, Hrsg., Dependability: Basic Concepts and Terminology in English, French, German, Italian and Japanese, Wien: Springer Verlag, 1992.

[53] A. Knossel, „Sind wir schon da? Roboter-Autos mischen sich in den Verkehr,“ *c't,* Nr. 9, pp. 132-136, 7 4 2014.

[54] D. Dahlmann, „Da wollen wir hin. Technische und rechtliche Grundlagen für selbstfahrende Autos,“ *c't,* Nr. 9, pp. 140-142, 7 4 2014.

[55] A. Davies, "INFINITI’S NEW STEERING SYSTEM IS A BIG STEP FORWARD—UNLESS YOU LOVE CARS," 6 4 2014. [Online]. Available: http://www.wired.com/2014/06/infiniti-q50-steer-by-wire/.

[56] R. Lyons und W. Vanderkulk, „The Use of Triple-Modular Redundancy to Improve Computer Reliability,“ *IBM Journal of Research and Development , vol.6, no.2,* pp. 200-209, April 1962.

[57] H. Bischof, „Rechnersystem“. Deutschland Patent DE 42 19 457 A1, 1992.

[58] AK EGAS, „Standardisiertes E-Gas-Überwachungskonzept für Motorsteuerungen von Otto- und Dieselmotoren,“ Arbeitskreis EGAS, 2006.

[59] J. Peleska und O. Schulz, „Reliability Analysis of Safety-Related Communication Architectures,“ Bremen, 2010.

[60] Maihöfer, Daimler AG, „Implementierung von Kommunikationsverbindungen in sicherheitsrelevanten Fahrzeugsystemen,“ Sindelfingen, 2011.

[61] J. Edel, „Steuersystem zum sicheren Betreiben von mindestens einer Funktionskomponente“. Deutschland Patent DE 10 2009 019 792, 2009.

[62] J. Edel, „Winkelvermessung mehrperiodischer Kreisbewegungen mit einem Hall-Sensor für dreidimensionale Anwendungen, Masterarbeit an der Fernuniversität Hagen,“ Hagen, 2012.

[63] Melexis Ltd., „MLX90363 Rotary Position Sensor IC feat. Hi-Speed Serial Interface. Datasheet 3901090363 Rev. 00W for component MLX90363," Tessenderlo, 2010.

[64] Leopold KOSTAL GmbH & Co. KG, Lenksäulenmodule, Kundenmehrwert durch Mechatronikintegration. Die Bibliothek der Technik (BT) 337, Süddeutscher Verlag Onpact, 2011.

[65] G. Ebner, J. Gutow, A. Koch und D. Weisser, „Lenkwinkelsensor, insbesondere für ein Kraftfahrzeug". Patent DE 10 2008 033 236, 2008.

[66] Wikipedia, „Hauptseite von Wikipedia," 2013. [Online]. Available: http://de.wikipedia.org/wiki/.

[67] Hella KGaA Hueck & Co., „Products & Services: Sensors," 14 Oktober 2014. [Online]. Available: http://www.hella.com/hella-com/504.html?rdeLocale=en.

[68] Hella KGaA Hueck & Co., „Position MeasureMent by CiPos® - HELLA," 21 10 2014. [Online]. Available: www.hella.com/microsite-electronics/.../06_CIPOS_gb_druck.pdf.

[69] J. Edel, W. Thormann und R. Bühlmann, „Drehwinkelmessvorrichtung". Deutschland Patent DE 10 2010 053 596, 2010.

[70] J. Edel, „Drehwinkelmessvorrichtung". Deutschland Patent DE 10 2010 019 508, 2010.

[71] J. Edel, „Vorrichtung zur Winkelmessung in mehrperiodischen Kreisbewegungen". Deutschland Patent DE 10 2012 014 876, 2012.

[72] J. Edel, „Rechnersystem zur Auswertung sicherheitskritischer Sensorgrößen". Deutschland Patent DE 10 2008 003 515, 2008.

[73] NASA, *Software Safety Guidebook. NASA Technical Standard*, 2004.

[74] ISO, *ISO/IEC 9899 - Programming Languages -- C*, 1990.

[75] ISO, „ISO 9001, Qualitätsmanagementsysteme – Anforderungen," 2008.

[76] ISO/VDA, „ISO/TS 16949:2009 Qualitätsmanagementsysteme. Besondere Anforderungen bei Anwendung von ISO 9001:2008 für die Serien- und Ersatzteilproduktion in der Automobilindustrie," 2009.

[77] M. Krüger, „Testen von Software als analytische Massnahme der Software-Qualitätssicherung," 1990.

[78] C. Gebauer, „ISO 26262 - status and roadmap," in s *6th International Annual Conference ISO26262*, Stuttgart, 2014.

[79] „AUTOSAR: Technical Safety Concept Status Report,“ Autosar Consortium, 2009. [Online]. Available: AUTOSAR_TR_SafetyConceptStatusReport.pdf.

[80] ISO/IEC, *ISO/IEC 19501, Information technology – Open Distributed Processing – Unified Modeling Language (UML),* 2005.

[81] P. Koopman und T. Chakravarty, „Cyclic Redundancy Code (CRC) Polynomial Selection for Embedded Networks,“ in s *The International Conference on Dependable Systems and Networks, DSN-2004,* Pittsburgh, USA, 2004.

[82] T. Baicheva, S. Dodunekov und P. Kazakov, On the cyclic redundancy-check codes with 8-bit redundancy, Bd. Volume 21, Computer Communications, 1998, pp. 1030-1033.

## EIDESSTATTLICHE ERKLÄRUNGEN

Hiermit versichere ich, dass ich die vorliegende Dissertation eigenständig verfasst und keine anderen als die genannten Quellen und Hilfsmittel verwendet habe. Wörtliche oder annähernd wörtliche Zitate wurden von mir in angemessener Form und unter Angabe der entsprechenden Quelle kenntlich gemacht. Ich bin der Alleinautor ohne Koautorenschaft.

Ich erkläre hiermit, dass ich mich bisher keiner weiteren Doktorprüfung unterzogen habe. Ich habe die Dissertation in der gegenwärtigen oder einer anderen Fassung an keiner anderen Fakultät eingereicht.

_____ _____

Ort, Datum Jan Edel